UCLouvain

Faculté de droit et de criminologie

La reconnaissance faciale dans l'espace public : le cadre juridique actuel permet-il de justifier la surveillance des individus au nom de la sécurité publique ?

Auteure : Vanessa TETERINA
Promoteur : Bernard MOUFFE
Année académique 2022-2023
Master en droit – Finalité : Justice civile et pénale

Plagiat et erreur méthodologique grave

Le plagiat, fût-il de texte non soumis à droit d'auteur, entraîne l'application de la section 7 des articles 87 à 90 du règlement général des études et des examens.

Le plagiat consiste à utiliser des idées, un texte ou une œuvre, même partiellement, sans en mentionner précisément le nom de l'auteur et la source au moment et à l'endroit exact de chaque utilisation*.

En outre, la reproduction littérale de passages d'une œuvre sans les placer entre guillemets, quand bien même l'auteur et la source de cette œuvre seraient mentionnés, constitue une erreur méthodologique grave pouvant entraîner l'échec.

* A ce sujet, voy. notamment **http://www.uclouvain.be/plagiat**.

Remerciements

Tout d’abord, j’aimerais exprimer ma gratitude envers mon promoteur, Bernard Mouffe, dont les conseils, l'expertise et la disponibilité ont joué un rôle déterminant dans l’aboutissement de ce travail académique.

Je souhaite également remercier chaleureusement mes amis qui ont été présents à chaque étape de cette aventure et qui n’ont cessé de me remonter le moral dans les moments de doute et de difficulté. Je tiens à réserver une reconnaissance toute particulière à Baptiste Joachim, dont les longues heures de relecture attentive ont grandement contribué à la qualité finale de ce mémoire.

Enfin, je ne saurais oublier de mentionner ma maman, dont le soutien inconditionnel a été une source de motivation à chaque étape de ce travail.

TABLE DES MATIERES

INTRODUCTION **1**

TITRE 1. CONTEXTUALISATION DE LA RECONNAISSANCE FACIALE **4**

CHAPITRE 1. EXPLORATION DES CONCEPTS ESSENTIELS 4

Section 1. La biométrie 4

Section 2. La reconnaissance faciale 6

Section 3. L'espace public 9

CHAPITRE 2. DE QUELQUES UTILISATIONS ET BÉNÉFICES 10

Section 1. Sécurité et contrôle d'accès 11

Section 2. Domaine de la santé 13

CHAPITRE 3. LES VISAGES À NU : LES APPRÉHENSIONS DE LA RECONNAISSANCE FACIALE DANS L'ESPACE PUBLIC 14

Section 1. Risque d'erreurs et discriminations 14

Section 2. Intrusion dans la vie privée 17

Section 3. Risque de surveillance de masse 18

TITRE 2. CADRE JURIDIQUE DE LA RECONNAISSANCE FACIALE **22**

CHAPITRE 1. UN LABYRINTHE LÉGISLATIF : LA RECONNAISSANCE FACIALE ET L'UNION EUROPÉENNE 22

Section 1. À la croisée des règlements 23

Section 2. Disparités entre États membres 30

CHAPITRE 2. VERS UNE RÉGLEMENTATION EUROPÉEENNE DE LA RECONNAISSANCE FACIALE – L' « *AI ACT* » 31

Section 1. Contexte et objectifs 31

Section 2. Contrôle par la gestion des risques 32

Section 3. La reconnaissance faciale sous l'*AI Act* 34

Section 4. Vers une interdiction absolue ? 35

CHAPITRE 3. RÈGLES APPLICABLES AU NIVEAU NATIONAL 37

Section 1. La loi relative à la protection des données 37

Section 2. Loi sur la fonction de police et loi caméras 39

Section 3. Position de l'Autorité de protection des données 42

Section 4. Perspectives législatives 43

TITRE 3. ILLUSTRATION DES AFFAIRES RÉCENTES 45

CHAPITRE 1. L'AFFAIRE BRUSSELS AIRPORT 45

Section 1. Utilisation de la reconnaissance faciale par la LPA 45

Section 2. Bases légales et rapport de l'Organe de contrôle 46

CHAPITRE 2. L'AFFAIRE *CLEARVIEW AI* 48

Section 1. L'application controversée – *Clearview AI* 48

Section 2. L'utilisation de l'application par la police judiciaire fédérale 49

Section 3. Analyse légale de l'affaire 50

Section 4. Comparaison avec l'affaire Brussels Airport 54

Section 5. Conclusion de *Clearview AI* 55

CONCLUSION 57

BIBLIOGRAPHIE 61

INTRODUCTION

« *L'appréhension du numérique par le droit est source d'indéniables défis pour le juriste* »[1]. Ce dernier, en quête de clarification et de rationalisation, n'est pas toujours apte à comprendre les notions et les subtilités « obscures » provenant du domaine informatique[2]. Aujourd'hui, de nombreux débats se concentrent sur les technologies biométriques qui inquiètent autant qu'elle fascinent, surtout lorsque ces technologies sont utilisées à des fins d'identification d'un individu[3] comme le font les systèmes de reconnaissance faciale. De plus en plus présents au sein de l'Union européenne, ces systèmes permettent notamment de vérifier, si un visage présenté dans les lieux publics correspond à une des images stockées dans une base de données, grâce à l'utilisation d'algorithmes[4]. Bien que certains États membres reconnaissent tout l'intérêt de cette nouvelle technologie, cette dernière suscite néanmoins d'intenses controverses dans le contexte politique et, en général, au sein de la société.

En effet, même s'il existe de réels avantages à appliquer ces technologies à des fins sécuritaires, le fait qu'elles aient un caractère intrusif et qu'elles engendrent encore énormément d'erreurs suscite un certain nombre de préoccupations quant à leur efficacité réelle[5], leur degré d'atteinte aux droits fondamentaux, notamment le droit au respect de la vie privée[6], ainsi qu'aux valeurs éthiques essentielles que sont « la dignité, l'autonomie et la justice sociale »[7]. Ainsi, nous nous retrouvons dans une situation assez contrastée avec d'un côté des fournisseurs de technologies de reconnaissance faciale de plus en en plus performants qui arrivent très souvent à persuader les politiciens de leur efficacité à améliorer la sécurité publique et de l'autre des chercheurs ou des régulateurs qui « tirent la sonnette d'alarme »[8]. En effet, une fois que les images sont enregistrées et analysées, il n'y a aucun moyen de garantir que le système ne puisse

---

[1] J. EYNARD, « Titre II - Le cadre juridique d'un schéma d'identification protecteur des droits et libertés », *L'identité numérique*, 1e édition, Bruxelles, Larcier, 2020, p. 161. ; Les références et citations du présent mémoire sont conformes aux règles méthodologiques utilisées dans l'ouvrage de N. BERNARD (dir.), *Guide des citations, références et abréviations juridiques*, 6e éd., Bruxelles, Kluwer, 2017.
[2] J. EYNARD, *ibidem*, p. 161.
[3] J. EYNARD, *ibidem*, p. 161.
[4] CNIL, « Reconnaissance faciale », disponible sur https://www.cnil.fr/fr/definition/reconnaissance-faciale, *s.d.*, consulté le 8 août 2023.
[5] D. SCHOENHER, « Reconnaissance faciale et contrôles préventifs sur la voie publique, l'enjeu de l'acceptabilité », *Les Notes du CREOGN,* 2019, N° 43, p. 1.
[6] T. MADIEGA et H. MILDEBRATH, « Réglementation de la reconnaissance faciale au sein de l'Union européenne », *EPRS*, septembre 2021, p. 1.
[7] Y. POULLET, *Le RGPD face aux défis de l'intelligence artificielle*, 1ère édition, Bruxelles, Larcier, 2020, p. 9 et 10.
[8] C. CASTELLUCCIA et D. LE MÉTAYER, « Analyse des impacts de la reconnaissance faciale - Quelques éléments de méthode », *Inria*, 2019, p. 4.

pas être abusé ou créer des effets indésirables. C'est pour cela qu'il est nécessaire de mettre en place des mesures juridiques qui obligent les fournisseurs de nouvelles technologies à rendre des comptes de leurs utilisations et garantir leur sécurité[9].

Consciente de cette nécessité, l'Union européenne a adopté le Règlement général sur la protection des données à caractère personnel et à la libre circulation de ces données, dit également « RGPD »[10], dont le but est de protéger les libertés et les droits des individus « face à l'utilisation de plus en plus fréquente de leurs données à caractère personnel »[11]. Le cadre législatif reste cependant flou quant aux institutions qui peuvent contrôler ou autoriser les systèmes de surveillance biométrique[12]. Par conséquent, on retrouve divers acteurs qui remettent en question l'efficacité du cadre juridique actuel de l'Union. Yves Poullet, ancien directeur du Centre de recherches informatique et droit (CRID), est convaincu que la réglementation actuelle « souffre de lacunes » et que « le RGPD n'offre pas toujours le bon angle d'attaque aux problèmes que soulève l'intelligence artificielle »[13].

Dans ce contexte, la Commission européenne a publié en avril 2021[14] une proposition de loi européenne sur l'intelligence artificielle qui vise à harmoniser les règles des États membres en matière de systèmes d'identification biométrique et introduire de nouvelles règles régissant l'utilisation des technologies de reconnaissance faciale au sein de l'Union[15]. La proposition prévoit notamment de classer les différentes technologies en trois catégories de risques : risques inacceptables, élevés et minimes[16]. La Commission stipule que toutes les applications ne sont pas menaçantes pour nos libertés démocratiques : certaines comportent trop de risques de porter atteinte aux droits fondamentaux et ne devraient donc jamais être autorisés, certaines sont des applications à « haut risque » qui peuvent survenir dans certaines circonstances avec des protections et des garanties évidentes, et enfin certaines sont des utilisations banales des technologies qui nécessitent moins d'attention. Dès lors, une évaluation

[9] C. CASTELLUCCIA et D. LE MÉTAYER, *ibidem*, p. 4.
[10] Règlement (UE) 2016/679 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 dir. 95/46/CE, *J.O.U.E.*, 27 avril 2016 (ci-après abrégé « R.G.P.D. »).
[11] J. EYNARD, *op. cit.,* p. 162.
[12] F. RAGAZZI *et al*., « Biometric & Behavioural Mass Surveillance in EU Member States », disponible sur www.greens-efa.eu/biometricsurveillance/, 1 octobre 2021, p. 12.
[13] Y. POULLET, *op. cit*., p.10.
[14] Proposition de règlement (UE) 2021/0106 du Parlement européen et du Conseil du 24 avril 2021 établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union.
[15] T. MADIEGA et H. MILDEBRATH, *op.cit.,* résumé.
[16] F. RAGAZZI *et al*., *op.cit.,* p. 8.

des aspects éthiques et juridiques de ces différents niveaux de dangerosité ne peut être dissociée « d'une compréhension fine du fonctionnement de ces technologies »[17].

Nous avons conscience que les questions que soulèvent les technologies de reconnaissance faciale dépassent le cadre du droit positif. Comme l'a souligné Wojciech Wiewiórowski, le contrôleur européen de la protection des données, « se focaliser sur les enjeux de vie privée serait une erreur. Il s'agit fondamentalement d'une question éthique pour une société démocratique »[18]. Toutefois, par souci de concision, nous ne attarderons pas sur cet aspect-là en détail. L'objectif de ce mémoire n'est donc pas de déterminer si une utilisation raisonnée de la reconnaissance faciale est encore possible mais bien d'examiner comment cette technologie est actuellement traitée en Europe, plus précisément en Belgique, en termes de législation afin de déterminer si celle-ci est adéquate et suffisamment encadrée pour garantir nos droits fondamentaux.

Avant de nous lancer dans le cœur du sujet, à savoir l'analyse du cadre juridique actuel de la reconnaissance faciale, nous devons d'abord présenter le contexte. Étant donné que nous utiliserons des termes techniques peu familiers, nous veillerons à les définir aussi clairement et précisément que possible. Dans un même temps, nous explorerons quelques utilisations que la technologie de reconnaissance faciale peut offrir, et expliquerons pourquoi cette nouvelle technologie comporte à la fois des avantages et des risques.

Nous nous pencherons ensuite sur la position du législateur à ce sujet, tant au niveau européen que national. Nous examinerons les règles qui sont utilisées pour encadrer et légitimer l'usage de telles technologies, ainsi que les initiatives législatives prises pour rester en phase avec les évolutions actuelles, notamment en considérant la proposition de loi européenne relative à l'intelligence artificielle. Toutefois, nous constaterons que le débat entre les différentes instances européennes se révèle bien plus complexe que prévu, entrainant des retards dans l'adoption de la loi.

Enfin, nous terminerons notre exposé par l'illustration de quelques affaires récentes qui se sont passées en Belgique et qui ont attiré toute notre attention.

---

[17] F. RAGAZZI *et al*., *ibidem,* p. 9.
[18] C. CASTELLUCCIA et D. LE MÉTAYER, *op. cit.*, p. 26. ; Traduction libre de W. WIEWIÓROWSKI, « Facial recognition: A solution in search of a problem? », disponible sur https://edps.europa.eu, 28 octobre 2019.

TITRE 1. CONTEXTUALISATION DE LA RECONNAISSANCE FACIALE

La reconnaissance faciale étant une technologie relativement complexe en termes d'utilisation des données biométriques, il est primordial de clarifier les notions élémentaires avant de se pencher sur le cœur du problème. C'est pourquoi le premier chapitre de ce mémoire sera consacré à une brève présentation de la technologie de reconnaissance faciale couplée a des caméras de surveillance. Celui-ci comprendra les définitions de certaines terminologies clés pertinentes pour ce mémoire et des explications sur son fonctionnement afin d'éviter d'éventuelles confusions avec d'autres technologies voisines. Dans le deuxième chapitre, nous aborderons certaines applications et bénéfices potentiels qu'une telle technologie peut apporter. Le troisième chapitre quant à lui, se focalisera sur les principales inquiétudes suscitées par l'utilisation de la reconnaissance faciale dans l'espace public[19].

CHAPITRE 1. EXPLORATION DES CONCEPTS ESSENTIELS

Section 1. La biométrie

L'article 4.14 du Règlement général sur la protection des données, dit « RGPD », définit les données biométriques comme étant « les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent son identification unique, telles que des images faciales ou des données dactyloscopiques »[20].

Ainsi, le Règlement distingue deux catégories d'informations qui peuvent être envisagées comme des données biométriques. D'un côté, nous avons les caractéristiques physiques ou physiologiques d'une personne physique. Cette catégorie est assez simple et correspond à ce que la majorité des personnes comprennent par « données biométriques », comme par exemple des informations relatives au visage, les empreintes digitales des doigts et du réseau veineux, les scans de l'iris ainsi que les analyses biologiques (ADN, salive, sang ou urine)[21].

De l'autre côté, nous retrouvons les caractéristiques comportementales, une catégorie considérablement plus large, englobant les traits de personnalité d'une personne, les habitudes,

[19] La structure de ce premier titre s'inspire en partie de la source suivante : T. MADIEGA et H. MILDEBRATH, *op.cit.*
[20] Art. 4.14 du R.G.P.D.
[21] T. MADIEGA et H. MILDEBRATH, *op. cit.*, p. 1.

les actions et les dépendances[22]. Cela inclut des informations comportementales qui permettent l'identification unique d'une personne, comme la reconnaissance vocale[23], une signature manuscrite ou même une façon de marcher[24]. La reconnaissance faciale qui nous intéresse en l'espèce, appartient elle, à la première catégorie.

Dès lors, on comprend en lisant l'article 4.14 du RGPD, que les données biométriques sont des données extrêmement sensibles car leur traitement peut comporter des risques significatifs pour les droits fondamentaux des personnes. En effet, comme ce sont des données permanentes et « hautement » personnelles, cela implique qu'une fuite de données peut avoir de dangereuses conséquences à long terme[25].

Il convient de souligner que la sensibilité d'une donnée peut être fortement influencée par le contexte dans lequel elle est utilisée, particulièrement lorsque cette donnée ne serait pas considérée comme sensible en toutes circonstances. Par exemple, une image faciale n'est, en soi, pas considérée comme une donnée sensible, mais si celle-ci est traitée pour déterminer l'origine raciale ou ethnique de la personne représentée, cette information devra être considérée comme sensible[26]. Le considérant 51 du Règlement précise notamment que photographies entrent dans la catégorie de données sensibles seulement « lorsqu'elles sont traitées selon un mode technique spécifique permettant l'identification ou l'authentification unique d'une personne physique »[27].

Ainsi, l'article 9.1 du RGPD[28] prévoit un régime plus « protecteur »[29] pour les données sensibles que pour les données ordinaires. En effet, c'est le principe de l'interdiction générale de traitements de données à caractère personnel qui prévaut, à moins que le responsable du traitement puisse invoquer « de manière cumulée une base juridique conformément à l'article 6 du RGPD et l'un des motifs d'exception énumérés à l'article 9.2 du RGPD »[30].

---

[22] FRA, « Facial recognition technology: fundamental rights considerations in the context of law enforcement », *Publications Office of the European Union*, 2020, p. 5.
[23] T. MADIEGA et H. MILDEBRATH, *op. cit.,* p. 1.
[24] FRA, *op. cit*., p. 5.
[25] Autorité de protection des données, « Recommandation relative au traitement de données biométriques », disponible sur www.autoriteprotectiondonnees.be, décembre 2021, p. 3 et 6.
[26] C. DE TERWANGNE, « Présentation générale du R.G.P.D. et des lois belges relatives à la protection des données », *Le Règlement général sur la protection des données (R.G.P.D./G.D.P.R.) : premières applications et analyse sectorielle*, Liège, Anthemis, 2020, p. 31.
[27] Considérant 51 du R.G.P.D.
[28] Art. 9.1 du R.G.P.D. « *le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits* ».
[29] C. DE TERWANGNE, *op. cit*., p. 32.
[30] Autorité de protection des données, *op. cit.*, p. 6. ; Ces différentes dispositions seront examinées dans le Titre 2.

Section 2. La reconnaissance faciale

En ce qui concerne la reconnaissance faciale, il n'existe pas de définition précise dans le cadre du RGPD. Toutefois, selon l'Autorité de protection des données, cette technologie est un système biométrique qui utilise les caractéristiques du visage pour deux fonctions principales à savoir l'authentification (§1) et l'identification (§2)[31] et comporte plusieurs modes de reconnaissance faciale tels que la reconnaissance de proximité ou à distance (§3), et la reconnaissance en temps réel ou a posteriori (§4)[32].

§1. Authentification

La fonction d'authentification de la reconnaissance faciale, également appelée « *one-to-one comparison* »[33], permet de comparer deux « gabarits biométriques »[34] présumés appartenir à la même personne, pour vérifier si la personne représentée sur les deux images est bien la même[35]. Cette fonction convient particulièrement aux situations où la personne est disposée à fournir volontairement des informations permettant de l'identifier, en comparant les informations de référence déjà établies avec les nouvelles données collectées[36].

Une utilisation fréquente de cette fonction d'authentification est notamment observée dans les aéroports pour les contrôles automatisés des frontières[37], où la personne scanne son passeport et fournit une image en direct pour être comparée à l'image du passeport. Pour que l'identité soit vérifiée, il est nécessaire que la probabilité de correspondance entre les deux images dépasse un certain seuil. En outre, il n'est pas obligatoire que les caractéristiques biométriques soient stockées dans une base de données, elles peuvent également être stockées sur une carte d'identité ou de voyage[38].

---

[31] Autorité de protection des données, « Reconnaissance faciale et droit à l'image », disponible sur www.autoritedeprotectiondesdonnees.be, s.*d.,* consulté le 2 mars 2023.
[32] R. WAELEN, « The struggle for recognition in the age of facial recognition technology », *AI and Ethics*, 2023, p. 216.
[33] Comparaison un-à-un ou correspondance biométrique.
[34] « *Un gabarit biométrique désigne les mesures qui sont mémorisées lors de l'enregistrement des caractéristiques morphologiques (empreinte digitale, forme de la main, iris...), biologiques (ADN, urine, sang...) ou comportementales (démarche, dynamique de tracé de signature...) de la personne concernée* ». Source : Commission nationale de l'Information et des Libertés, « Biométrie : un 'gabarit' biométrique, c'est quoi ? », disponible sur www.cnil.fr, *s.d.*, consulté le 2 mars 2023.
[35] FRA, *op. cit.*, p. 7.
[36] Autorité de protection des données, « Recommandation relative... », *op. cit.*, p. 15.
[37] Par exemple, le gouvernement britannique a mis en place des « eGates » dans 15 ports aériens et ferroviaires du Royaume-Uni : X, « Guide to faster travel through the UK border », disponible sur www.gov.uk, 2 mai 2023.
[38] FRA, *op. cit.*, p. 7.

§2. Identification

La fonction d'identification de la reconnaissance faciale, également appelée « *one-to-many comparison* »[39], consiste quant à elle, à comparer le modèle d'une image faciale d'une personne à plusieurs autres modèles stockés dans une base de données pour déterminer si son image y est présente. Cette comparaison génère un score qui indique la probabilité que les deux images correspondent à la même personne. Cette opération peut être effectuée avec une base de données connue (identification par ensemble fermé) ou inconnue (identification par ensemble ouvert)[40].

L'identification est souvent utilisée pour les listes de surveillance, où les images faciales sont obtenues à partir de caméras vidéo et comparées à une base de données de référence. Ces systèmes biométriques sont appelés technologies de reconnaissance faciale « en temps réel ». Cependant, la qualité des images obtenues à partir des caméras vidéo peut être limitée par la lumière, la position des personnes et la distance, ce qui augmente le risque de fausses correspondances[41]. Cette seconde fonction présente également des risques de fuite[42] plus importants en raison de la nécessité d'utiliser une base de données pour effectuer des comparaisons avec les images faciales, mais aujourd'hui, c'est l'utilisation la plus fréquente de la reconnaissance faciale dans le contexte de la répression[43].

Les opinions divergent quant à l'usage de la reconnaissance faciale dans les lieux publics. Certains, comme le maire de Nice, expriment leur mécontentement quant à l'impossibilité d'utiliser des solutions qui pourraient permettre l'identification des personnes fichées et ainsi prévenir des attaques terroristes[44]:

« Je demande à ce que le législateur fasse évoluer les textes, au rythme où évolue la société. Je dispose du logiciel qui permettrait dès demain matin d'appliquer la reconnaissance faciale et d'identifier des individus fichés où qu'ils se trouvent dans la ville... Pourquoi l'interdire ? Est-ce qu'on veut prendre le risque de voir des gens mourir au nom des libertés individuelles, alors qu'on a les technologies qui permettraient de l'éviter ? »[45].

---

[39] Comparaison un à plusieurs ; Autorité de protection des données, « Recommandation relative... », *op. cit.*, p. 15.
[40] FRA, *op. cit*., p. 7.
[41] FRA, *ibidem,* p. 8.
[42] C. CASTELLUCCIA et D. LE MÉTAYER, *op. cit*., p. 7.
[43] V. RAPOSO, « The use of facial recognition technology by law enforcement in Europe: a non-Orwellian draft proposal », *European Journal on Criminal Policy and Research*, 2022, p. 2.
[44] C. CASTELLUCCIA et D. LE MÉTAYER, *op. cit*., p. 3.
[45] G. ALLIX, « Comment des villes « hyper connectées » contrôlent l'espace public », *Le Monde*, disponible sur www.lemonde.fr, 19 décembre 2018.

D’autres, comme Wojciech Wiewiórowski, le contrôleur européen de la protection des données, font une distinction entre le recours à la reconnaissance faciale pour l’authentification, qui leur semble raisonnable, et son utilisation à des fins d’identification qui leur paraît beaucoup plus discutable[46] :

« Les objectifs qui ont déclenché l'introduction de la reconnaissance faciale peuvent sembler incontestables à première vue : il semble normal de l'utiliser pour vérifier l'identité d'une personne par rapport à une image faciale présentée, comme aux frontières nationales, y compris dans l'UE. Il s'agit d'un autre niveau d'intrusion que de l'utiliser pour déterminer l'identité d'une personne inconnue en comparant son image à une vaste base de données d'images d'individus connus »[47].

Ainsi, nous retrouvons deux positions opposées sur le sujet. D’un côté, les partisans de cette technologie qui mettent en avant son potentiel dans la lutte contre la criminalité en permettant l’identification et la recherche efficaces des criminels et de l’autre côté, les défenseurs de la protection de la vie privée qui expriment de sérieuses inquiétudes concernant les atteintes potentielles aux libertés individuelles. Au cœur de ce débat, nous avons l’éternelle question de l’équilibre entre sécurité et liberté. La reconnaissance faciale offre des avantages indéniables en matière de sécurité publique, mais dans un même temps, son utilisation à des fins répressives soulève des questions cruciales sur la protection de la vie privée et les droits fondamentaux. Nous verrons par la suite que la réglementation de cette technologie ne fait pas un simple choix binaire entre ces deux positions. Elle est élaborée avec une approche nuancée qui prend en compte les bénéfices potentiels de la technologie tout en fixant des limites claires pour protéger la vie privée des individus.

§3. Le reconnaissance faciale de proximité ou à distance

La Commission européenne dans sa proposition de loi européenne sur l’intelligence artificielle définit l’identification biométrique à distance comme « un système d’IA destiné à identifier des personnes physiques à distance par la comparaison des données biométriques d’une personne avec les données biométriques contenues dans une base de données de référence »[48].

[46] C. CASTELLUCCIA et D. LE MÉTAYER, *op. cit*., p. 7.
[47] Traduction libre de W. WIEWIÓROWSKI, *op. cit*.
[48] Proposition de règlement (UE) 2021/0106 du Parlement européen et du Conseil du 24 avril 2021 précitée, p. 22.

Ainsi, la reconnaissance faciale à distance peut permettre l'identification d'un individu dans la rue en analysant les séquences vidéo des caméras de surveillance. La reconnaissance faciale de proximité, quant à elle, n'est pas définie dans la proposition de loi, mais selon la doctrine, il est fort probable qu'elle inclue des dispositifs tels que des lunettes intelligentes ou une application pour téléphone qui permettraient à une personne d'identifier une autre personne dans le même lieu physique[49].

§4. La reconnaissance faciale en temps réel et a posteriori

La reconnaissance en temps réel et a posteriori concerne le moment auquel une personne est identifiée par un système biométrique. La reconnaissance en temps réel est basée sur l'utilisation d'éléments « en direct » ou « en léger différé », tandis que dans le cas de la reconnaissance a posteriori, les données biométriques sont d'abord stockées et la comparaison et l'identification ne sont effectuées qu'après un délai significatif[50].

Ces distinctions sont de conséquence, étant donné que les décideurs politiques traitent distinctement les différents modes de reconnaissance faciale. La proposition de loi européenne sur l'intelligence artificielle préconise l'interdiction de l'identification biométrique à distance et en temps réel dans les lieux publics. Cela implique que les technologies de reconnaissance faciale utilisés à proximité, a posteriori ou dans des espaces privés seraient toujours autorisés[51].

Section 3. L'espace public

La notion d'espace public constitue un point central de notre sujet, car notre attention se porte bien sur la reconnaissance faciale dans les lieux publics et non dans des contextes privés. Ainsi, pour déterminer précisément qu'est-ce qu'un espace public, la Commission européenne, dans sa proposition de loi européenne sur l'intelligence artificielle, définit à l'article 3 (39) l'espace public comme « tout espace physique accessible au public, indépendamment de l'existence des conditions d'accès à cet espace »[52].

La définition reste assez large et pour en savoir d'avantage il faut consulter le considérant 9 qui précise que les espaces publics sont tous les endroits physiques ouverts au public, que ceux-ci soient la propriété d'un individu privé ou d'une entité publique. Ainsi, la

[49] R. WAELEN, *op. cit.*, p. 216.
[50] Proposition de règlement (UE) 2021/0106 du Parlement européen et du Conseil du 24 avril 2021 précitée, p. 22.
[51] R. WAELEN, *op. cit.*, p. 216.
[52] Proposition de règlement (UE) 2021/0106 du Parlement européen et du Conseil du 24 avril 2021 précitée, art. 3 (39).

Commission explique que les lieux qui sont par nature privés et qui ne sont pas ouverts librement à des tiers, tels que les bureaux, les entrepôts, les résidences, les clubs privés et les usines ne sont pas couverts par cette notion, sauf si les tiers ont été expressément autorisés ou invités. Les espaces en ligne ne sont pas non plus inclus dans la définition.

Toutefois, la simple exigence de conditions d'accès à un lieu comme par exemple l'achat d'un billet d'entrée ou des restrictions d'âge, ne signifie pas que l'espace n'est pas accessible au public. Ainsi, en plus des espaces publics tels que les rues, les bâtiments publics et les infrastructures de transport, les lieux tels que les théâtres, cinémas et les centres commerciaux sont généralement considérés comme accessibles au public. Le considérant 9 précise cependant, que le statut d'accessibilité d'un espace au public doit être évalué au cas par cas, en prenant en considération les spécificités de chaque situation[53].

CHAPITRE 2. DE QUELQUES UTILISATIONS ET BÉNÉFICES

Les technologies de reconnaissance faciale sont utilisées dans divers contextes, que ce soit dans la sphère privée ou publique. Bien qu'elles soient devenues populaires auprès des consommateurs, des entreprises et des gouvernements[54], leur utilisation doit être surveillée pour éviter toute violation des droits fondamentaux des individus.

Si l'on parcourt les différentes utilisations potentielles de cette technologie biométrique, il est possible de les classer en fonction du degré de contrôle que les individus ont sur leurs données personnelles, de leur liberté de décider d'utiliser cette technologie, des conséquences qu'elle entraine pour eux et de l'ampleur des traitements impliqués[55]. Il est évident que l'utilisation de la reconnaissance faciale sur un support individuel à des fins personnelles ne suscite pas les mêmes enjeux et conséquences qu'un usage dans un espace public à des fins d'identification, sans le consentement des individus. Il existe donc une large gamme de nuances entre ces deux extrêmes[56].

Sans prétendre offrir une liste exhaustive des contextes dans lesquels la reconnaissance faciale peut être utilisée, on peut notamment citer les cas d'usages expliqués ci-après.

---

[53] Proposition de règlement (UE) 2021/0106 du Parlement européen et du Conseil du 24 avril 2021 précitée, considérant 9.
[54] T. MADIEGA et H. MILDEBRATH, *op. cit.*, p. 3.
[55] CNIL, « Reconnaissance faciale - pour un débat à la hauteur des enjeux », disponible sur www.cnil.fr, 15 novembre 2019, p. 4.
[56] CNIL, *ibidem*, p. 4.

Section 1. Sécurité et contrôle d'accès

Lorsque nous évoquons les technologies de reconnaissance faciale dans les espaces publics, une des premières choses qui nous vient à l'esprit est leur capacité à renforcer la sécurité.

En premier lieu, ces technologies ont le potentiel de pouvoir prévenir et résoudre des crimes graves tels que des attaques terroristes[57], des meurtres ou des agressions, en permettant l'identification des suspects à partir d'images de vidéosurveillance. En outre, elles pourraient prévenir des infractions de moindre gravité, telles que la fraude en identifiant plus efficacement les personnes qui utilisent de faux documents d'identité[58]. Ces technologies pourraient même avoir un effet dissuasif, en empêchant les personnes qui souhaitent commettre un délit de passer à l'acte car elles seront conscientes d'être surveillées. Toutefois, évaluer l'impact de ces technologies sur la population criminelle, ou sur la population en général, reste relativement difficile[59].

L'institut Ada Lovelace au Royaume-Uni, a mené une étude[60] portant sur l'acceptabilité de la reconnaissance faciale auprès de 4109 personnes âgées de 16 ans ou plus. L'objectif était d'évaluer la perception des individus à l'égard de cette technologie. Selon le rapport, il apparait que le public fait une balance entre les avantages en matière de sécurité, ainsi que les limites à mettre en place pour éviter le risque d'une surveillance de masse. Ainsi, on constate que plus de 80% des participants ont considéré que la reconnaissance faciale était bénéfique et contribuait à la sécurité de la société. En outre, 71% des sondés ont estimé que la police devrait pouvoir utiliser la reconnaissance faciale dans l'espace public, à condition que cela contribue à réduire la criminalité[61]. Nous pouvons donc en déduire que la majorité des participants de l'étude ont exprimé une vision globalement positive de la reconnaissance faciale en termes d'avantages pour la sécurité publique, mais que la mise en place de garde-fous et de réglementations reste essentielle pour prévenir les abus potentiels et préserver la vie privée des individus.

---

[57] M. SMITH et S. MILLER, « The ethical application of biometrical recognition technology », *AI & Society,* Brighton*,* 2022, p. 173.
[58] M. SMITH et S. MILLER, *ibidem*, p. 173.
[59] L. MUCCHIELLI, « Note sur l'évaluation des nouvelles technologies de sécurité. Cas de la vidéosurveillance et de la reconnaissance faciale », *Laboratoire Méditerranéen de Sociologie*, 2019, p. 5.
[60] ADA LOVELACE INSTITUTE, « Beyond face value: public attitudes to facial recognition technology », disponible sur www.adalovelaceinstitute.org, septembre 2019.
[61] M. KIMRI, P. LEGROS et C. LEQUESNE ROTH, « La Reconnaissance Faciale dans l'espace public – Une cartographie européenne », *Rapport de la Fablex DL4T*, avril 2020, p. 45.

En deuxième lieu, la sécurité concerne également le contrôle d'accès à des lieux publics, des outils ou des services. En effet, les technologies biométriques placées dans certains lieux comme un bureau d'entreprise, une école ou une chambre d'hôtel[62], permettraient de donner accès uniquement aux personnes qui ont le droit d'y accéder, ou encore d'autoriser une personne en particulier à utiliser un outil comme un distributeur de billets à la banque qui reconnaitrait ses clients[63]. De plus, la reconnaissance faciale peut être utilisée pour contrôler l'accès et identifier les individus en temps réels lors de rassemblements publics tels que des manifestations, des concerts ou des évènements sportifs[64].

Nous pouvons notamment citer le cas du stade *Racing White Daring Molenbeek* qui a commencé à expérimenter la technologie de reconnaissance faciale en 2019, en permettant aux supporters du club d'entrer plus facilement dans le stade par le biais de la file prioritaire. « Il s'agira d'un couloir réservé aux supporters qui ont accepté de participer au projet. Il sera lui-même muni de ces caméras intelligentes et leur ouvrira directement la porte d'accès au stade en reconnaissant leur visage. De quoi gagner de précieuses minutes par exemple lorsqu'on arrive tout juste avant le coup d'envoi »[65], expliquait Jean-Marie Marinus, l'un des responsables du projet. La légitimité de cette expérimentation repose sur le consentement des participants, car seuls les supporters ayant accepté de participer verront leur visage authentifié[66]. Pour assurer la confidentialité, des mesures techniques ont été mises en place. Les photos scannées ainsi que les visages associés aux noms des participants sont stockés sur un serveur interne au stade qui n'est pas connecté à Internet ou à d'autres systèmes. Seul le personnel autorisé a accès à ces données, qui ne sont ni transmises à des tiers, ni croisées avec d'autres bases de données[67]. De plus, il est possible pour un supporter de retirer son consentement à tout moment et mettre fin à sa participation à l'expérience en faisant une demande en ligne. Si le supporter ne se réabonne pas, ses données sont tout simplement effacées au bout d'un mois[68].

Il convient de souligner que l'Autorité de protection des données personnelles n'a donné aucun avis sur ce cas d'usage et qu'aucune analyse d'impact n'a été publiée, ou peut-être même,

[62] CEST, « Les enjeux éthiques soulevés par la reconnaissance faciale », 8e commission jeunesse, disponible sur www.ethique.gouv.qc.ca, 2020, p. 11.
[63] CNIL, « Reconnaissance faciale – pour un débat... », *op. cit*., p. 4.
[64] T. MADIEGA et H. MILDEBRATH, *op. cit*., p. 4.
[65] B. SCHMITZ, « Le RWDM comme laboratoire pour une technologie de reconnaissance faciale », disponible sur www.rtbf.be, 5 septembre 2018.
[66] M. KIMRI, P. LEGROS et C. LEQUESNE ROTH, *op. cit.*, p. 65
[67] B. SCHMITZ, *op. cit.*
[68] M. KIMRI, P. LEGROS et C. LEQUESNE ROTH, *op. cit.*, p. 65.

n'a jamais été faite. Nous remarquons donc un manque de transparence concernant cette utilisation[69].

Section 2. Domaine de la santé

Les services hospitaliers pourraient se prémunir de la reconnaissance faciale afin de détecter certaines maladies dont les symptômes affectent le visage, y compris des maladies psychiatriques telles que la dépression, en identifiant des détails qui ne sont pas toujours perceptibles à l'œil nu[70]. Les hôpitaux pourraient également recourir à ces technologies biométriques pour adapter le dosage des médicaments en fonction du temps et de chaque patient[71], en particulier pour suivre des patients âgés et s'assurer qu'ils prennent leurs médicaments de manière sûre et efficace[72].

Dans son rapport étudiant l'impact des exigences réglementaires en matière d'intelligence artificielle en Europe[73], la Commission européenne précise tout de même que la supervision humaine est essentielle pour contrôler le logiciel de reconnaissance faciale. Lorsqu'on met à jour un logiciel en le calibrant, un nouveau protocole d'évaluation est nécessaire. Les coûts, les risques et les incertitudes doivent être identifiés pour chaque application individuelle. Les développeurs ont donc la responsabilité de surveiller l'évolution de leurs algorithmes et de signaler aux organismes compétents tout changement inattendu ou indésirable. Bien que les risques varient en fonction de l'application, il est crucial de surveiller les sources de données pendant la phase de développement, ainsi que d'assurer une surveillance humaine pendant la phase de déploiement[74].

Comme précisé antérieurement, on a cité dans cette section seulement quelques utilisations qu'englobe la reconnaissance faciale constatées en Europe, et dont la conformité avec le RGPD ou d'autres lois n'a donc peut-être pas été vérifiée[75]. Il est important de souligner que dans d'autres pays, les utilisations potentielles de ces technologies biométriques peuvent être beaucoup plus vastes. En Chine[76] par exemple, la reconnaissance faciale est notamment utilisée pour identifier les personnes traversant au feu rouge, permettant ainsi de les sanctionner.

---

[69] M. KIMRI, P. LEGROS et C. LEQUESNE ROTH, *ibidem*, p. 65.
[70] CEST, *op. cit.,* p. 11.
[71] Commission européenne, « Study to Support an Impact Assessment of Regulatory Requirements for Artificial Intelligence in Europe. Final Report (D5) », disponible sur http://commission.europa.eu, avril 2021, p. 73.
[72] CEST, *op. cit*., p. 11.
[73] Commission européenne, « Study to Support an Impact... », *op. cit.*
[74] Commission européenne, *ibidem*, p. 74.
[75] CNIL, « Reconnaissance faciale – pour un débat... », *op. cit*., p. 5.
[76] CEST, *op. cit*., p. 12.

Dans ce contexte, il est nécessaire de raisonner au cas par cas afin de déterminer la légalité d'un traitement de données personnelles. Pour ce faire, il est essentiel de partir de la finalité du traitement afin d'évaluer la pertinence, la proportionnalité, la durée de conservation des données, la sécurité, etc. Bien que certains usages de la reconnaissance faciale soient légitimes, il est important de ne pas conclure que toute utilisation serait souhaitable ou réalisable[77].

CHAPITRE 3. LES VISAGES À NU : LES APPRÉHENSIONS DE LA RECONNAISSANCE FACIALE DANS L'ESPACE PUBLIC

Comme cela a déjà été évoqué à maintes reprises, les adeptes de la technologie de reconnaissance faciale vantent ses capacités miraculeuses à fonctionner de manière autonome pour effectuer des tâches complexes comme l'identification des suspects, et à produire des résultats incontestables même dans des conditions irréalistes[78]. Pourtant, la reconnaissance faciale soulève de nombreux problèmes en termes de droits fondamentaux qu'on parcourra de manière non-exhaustive dans le cadre de ce mémoire. Tour d'abord, nous constaterons qu'il existe de réelles préoccupations quant à la précision de la reconnaissance faciale, en particulier en ce qui concerne la reconnaissance de visages de différentes races et ethnies, ce qui peut entrainer des discriminations et des erreurs judiciaires (section 1). Nous noterons également que ce système biométrique viole la vie privée des individus car ces derniers peuvent être identifiés et suivis à leur insu (section 2). Enfin, nous évaluerons les éventuels dangers liés à l'utilisation de la technologie de reconnaissance faciale en raison de son potentiel de surveillance de masse (section 3).

Section 1. Risque d'erreurs et discriminations

La préoccupation la plus fréquemment évoquée en matière de reconnaissance faciale concerne les risques d'erreurs lorsqu'on compare des visages[79]. En effet, des recherches menées par des scientifiques[80] indiquent que la plupart des systèmes de reconnaissance faciale ont des performances techniques limitées, ce qui peut entrainer deux types d'erreurs : un faux positif lorsque le système identifie à tort un élément comme étant un visage et un faux négatif lorsque le système ne détecte pas un visage présent sur une image. Les taux d'erreur peuvent être élevés,

[77] CNIL, « Reconnaissance faciale – pour un débat... », *op. cit*., p. 5.
[78] M. JACQUET et L. GROSSRIEDER, « Enjeux et perspectives de la reconnaissance faciale en sciences criminelles », *Image et Justice*, Vol. 54, 2021, p. 150.
[79] M. O'FLAHERTY, « Facial recognition technology and fundamental rights », *EDPL*, 2020, p. 171.
[80] P. GROTHER, M. NGAN et K. HANAOKA, « Facial Recognition Vendor Test (FRVT). Part 3: Demographic Effects », *NLST*, 2019.

surtout lorsque les images comparées ont des arrière-plans, poses, éclairages ou ombres différents. En outre, les technologies de reconnaissance faciale sont moins précises lorsqu'il y a un grand écart d'âge entre les différentes images comparées[81] ou encore lorsque les individus ont des jumeaux[82].

En dépit de l'amélioration constante de la précision des systèmes de reconnaissance faciale, lorsqu'un grand nombre de personnes sont analysées, même une faible marge d'erreur peut entraîner un nombre inquiétant d'erreurs d'identification. Pour qu'un système fonctionnant à l'échelle de la population de l'Union européenne commette moins de 10 erreurs sur un total de 446 millions d'individus, il devrait avoir un taux d'erreur de seulement 0,00000224%, ce qui équivaut à une précision de 99,99999776%[83]. Cependant, même les systèmes de reconnaissance faciale les plus modernes ne sont pas encore capables d'atteindre de telles performances. En outre, plus la population cible est importante, plus le pourcentage d'erreur sera élevé[84].

À l'heure actuelle, la majorité des systèmes de reconnaissance faciale ont des taux de précision différents en fonction de l'origine ethnique, du sexe et de l'âge de la personne identifiée avec des performances souvent moins bonnes lorsqu'il s'agit de personnes aux peaux sombres et, en particulier, de femmes noires[85]. On peut citer deux raisons à cela. Premièrement, si une base de données ne contient pas suffisamment d'informations sur un groupe en particulier, les décisions prises à leur sujet risquent d'être moins fiables[86], avec des résultats biaisés qui peuvent donner lieu à une discrimination[87]. Deuxièmement, les programmeurs, souvent des hommes blancs, sont eux aussi biaisés[88] car ce sont eux qui choisissent quels codes transcrire et quelles variables utiliser ou ignorer. En effet, les algorithmes utilisés en intelligence artificielle ont tendance à refléter les préjugés sociaux des personnes qui les ont conçus. Ces préjugés peuvent être intentionnels, toutefois ils se reflètent dans les algorithmes[89]. Des études ont montré que cela pourrait être lié au fait que les ingénieurs sont plus motivés et attentifs

[81] T. MADIEGA et H. MIDERLBRATH, *op. cit*., p. 7.
[82] F. NOROOZI et O. TOYGAR, « Recognition of identical twins using fusion of various facial feature extractors », *EURASIP Journal on Image and Video Processing*, 2017, p. 1.
[83] V. RAPOSO, « When facial recognition does not 'recognise': erroneous identifications and resulting liabilities », *AI & Society*, 2022, p. 3.
[84] V. RAPOSO, *ibidem*, p. 3.
[85] P. GROTHER, M. NGAN et K. HANAOKA, *op. cit*.
[86] C. CASTETS-RENARD et P. BESSE, « Responsabilité *ex ante* de l'AI Act : entre certification et normalisation, à la recherche des droits fondamentaux au pays de la conformité », *Un droit de l'intelligence artificielle : entre règles sectorielles et régime général*, 1ère édition, Bruxelles, Bruylant, 2023, p. 614.
[87] M. O'FLAHERTY, *op. cit*., p. 171.
[88] Plus précisément, les données dont se nourrissent les intelligences artificielles (qui sont ensuite utilisées par les programmeurs) sont biaisées par le fait qu'Internet n'ait pas été à la portée de tous.
[89] V. RAPOSO, « When facial recognition does not 'recognise'… », *op. cit*., p. 4.

lorsqu'ils disposent de meilleures données de formation[90]. Il va de soi que si les technologies de reconnaissance faciale sont utilisées de manière discriminatoire en arrêtant plus souvent par erreur des personnes appartenant à certains groupes ethniques, cela pourrait affecter négativement la confiance de ces groupes envers la police ou les fonctionnaires chargés de la gestion des frontières[91].

Il convient de souligner que, même si des efforts puissent être faits pour minimiser les biais[92], comme par exemple l'auto-configuration des algorithmes, il est impossible de les éliminer complètement en raison de la nature inhérente de cette technologie, même avec des avancées majeures dans ce domaine[93]. Ainsi, pour réduire les biais autant que possible, il est crucial de veiller à ce que les données utilisées soient suffisamment représentatives afin d'éviter toute forme de discrimination.

De plus, il est indispensable de vérifier les méthodes employées par l'intelligence artificielle pour prendre des décisions[94]. En effet, l'utilisation des technologies de reconnaissance faciale comporte le risque que ni les individus, ni les autorités publiques ne puissent comprendre comment et pourquoi le système biométrique a produit et est parvenu à un résultat particulier. C'est pourquoi, il peut être difficile d'évaluer et de prouver si une personne a été « injustement désavantagée » en raison de l'utilisation de ces systèmes d'intelligence artificielle, notamment lors d'une décision de recrutement ou de promotion, ou d'une demande d'aide publique[95].

L'État qui utiliserait des algorithmes d'apprentissage automatique pour prendre des décisions ayant des répercussions sur les droits des individus, pourrait être confronté à des difficultés en raison de l'obligation de l'État de motiver sa décision, conformément au concept d'État de droit. Or un algorithme qui prend des décisions dont les justifications sont difficilement compréhensibles, ne peut pas remplir efficacement cette exigence. Par conséquent, étant donné que le recours à ces technologies soulève plusieurs problèmes

---

[90] B. COWGILL et F. DELL'ACQUA, « Biased programmers? Or biased data? A field experiment in operationalizing AI ethics », *Columbia Business School Research Paper Forthcoming*, 2020.
[91] FRA, *op. cit.*, p. 28.
[92] « En statistique ou épidémiologie, un biais est une démarche ou un procédé qui engendre des erreurs dans les résultats d'une étude », disponible sur https://fr.wikipedia.org/wiki/Biais_(statistique), consulté le 13 août 2023.
[93] CNIL, « Reconnaissance faciale - pour un débat... », *op. cit*., p. 8.
[94] C. CASTETS-RENARD, « Titre 2 - Réglementation des systèmes d'intelligence artificielle », *Droit du marché unique numérique et intelligence artificielle*, 1e édition, Bruxelles, Bruylant, 2020, p. 342.
[95] COM(2021) 205, Communication de la Commission au Parlement européen, au Conseil au Comité économique et social européen et au Comité des régions, « Favoriser une approche européenne en matière d'intelligence européenne », Bruxelles, 21 avril 2021, p. 4.

complexes, il est crucial d'établir des règles cohérentes qui protègent les droits des individus tout en encourageant l'innovation[96].

Section 2. Intrusion dans la vie privée

La Commission européenne, dans un de ses rapports concernant les règlementations relatives à l'intelligence artificielle, met en avant les systèmes biométriques dites de la « deuxième vague », qui « déploient des technologies et des algorithmes plus élaborés collectant des données hautement sensibles et personnelles »[97]. Ces nouvelles pratiques soulèvent de sérieuses inquiétudes quant au respect du droit à la protection des données à caractère personnel établi à l'article 8 de la Charte des droits fondamentaux de l'Union européenne et au droit au respect de la vie privée et familiale énoncé à l'article 7 de la même charte[98]. Les préoccupations portent principalement sur la difficulté de garantir un consentement explicite des individus pour l'utilisation de ces technologies[99], parmi lesquelles on trouve la reconnaissance faciale.

Tout d'abord, la complexité intrinsèque des systèmes basés sur l'intelligence artificielle pose un enjeu majeur quant à la possibilité d'obtenir un consentement éclairé. Il est peu probable que des citoyens lambdas possèdent un niveau de connaissance adéquat sur le fonctionnement de ces systèmes et sur la manière dont leur utilisation peut interférer avec leur autonomie[100]. Ensuite, dans le domaine du numérique, les conditions d'utilisation sont souvent présentées dans des documents complexes qui sont rarement lus, ce qui soulève notamment des problèmes éthiques. Pour assurer la légitimité des actions des utilisateurs de ces technologies, maintenir la confiance du public et favoriser l'autonomie des personnes soumises à ces technologies, il est crucial que l'information soit accessible et compréhensible[101].

---

[96] A. KRACHLER, « La proposition du règlement sur l'intelligence artificielle – Vers une intelligence artificielle maîtrisée par l'humain ? », *Rev. Aff. Eur*., 2022/3, p. 499.

[97] « *La "deuxième vague" de biométrie déploie des technologies et des algorithmes plus élaborés, y compris l'analyse des ondes neurales, la luminescence de la peau, la lecture de l'iris à distance, la reconnaissance faciale avancée, la démarche, la parole, la biométrie comportementale, etc.*» in Commission européenne, « Study to Support an Impact... », *op. cit.* p. 39.

[98] Art. 7 et 8 de la Charte des droits fondamentaux de l'Union européenne, signée à Nice le 7 décembre 2000 (ci-après abrégée « Ch. dr. fond. UE »).

[99] T. MADIEGA et H. MILDEBRATH, *op. cit.*, p. 8.

[100] C. FONTES et C. PERRONE, « Ethics of surveillance: harnessing the use of live facial recognition technologies in public spaces for law enforcement », *IEAI*, 2021, p. 6.

[101] CEST, *op. cit*., p. 20.

Le consentement implique également l'existence de choix alternatifs et donc de pouvoir se retirer du système[102]. Cependant, si la technologie de reconnaissance faciale est déployée dans des zones où les individus doivent accéder pour leur vie quotidienne, cela peut compromettre leur autonomie de décision en mettant en péril leur droit d'accéder à l'espace public. Les choix peuvent sembler limités : accepter la surveillance pour accéder au lieu public en toute sécurité ou préserver sa vie privée au détriment de l'efficacité des actions policières. Il peut être difficile de considérer cela comme un véritable choix car refuser la surveillance pourrait être interprété comme un comportement suspect, et pourrait même mener à une éventuelle pénalité[103].

En outre, le consentement en matière de vie privée est un problème qui requiert une grande transparence. Les caméras, souvent discrètement intégrées dans le paysage urbain, constituent l'interface finale à laquelle les gens devront s'habituer. Si les systèmes de vidéosurveillance sont déjà mis en place, il peut être difficile pour les citoyens de remarquer toute amélioration dans le niveau de surveillance. Les personnes qui sont scannées ne sont peut-être pas conscientes qu'elles font l'objet d'un contrôle d'identité. Par conséquent, il est d'autant plus difficile d'obtenir leur consentement, car cela dépend fortement de l'accès à des informations « adéquates ». En l'absence d'informations et d'explications par les autorités publiques, un citoyen ne dispose que de très peu de moyens pour comprendre l'étendue et l'objectif de la surveillance exercée. Les caméras de surveillance confèrent donc un pouvoir considérable à ceux qui les utilisent[104].

Enfin, la limitation du droit à la vie privée et familiale par les technologies de reconnaissance faciale pourrait également avoir de graves conséquences à long terme. En effet, cela pourrait affecter le fonctionnement même de la démocratie, puisque « la vie privée est une valeur fondamentale inhérente à une société démocratique libérale et pluraliste, et une pierre angulaire de la mise en œuvre des droits fondamentaux »[105].

Section 3. Risque de surveillance de masse

Il existe de nombreuses craintes quant à une potentielle surveillance de masse due à l'utilisation de la reconnaissance faciale dans les espaces publics. La surveillance de masse peut

[102] P. FUSSEY et D. MURRAY, « Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology », *The Human Rights, Big Data and Technology Project*, 2019, p. 100.
[103] C. FONTES et C. PERRONE, *op. cit*., p. 7.
[104] C. FONTES et C. PERRONE, *ibidem,* p. 7.
[105] Traduction libre de M. O'FLAHERTY, *op. cit*., p. 171.

être définie comme « une forme de surveillance, de suivi ou de traitement des données personnelles (biométriques et comportementales) des individus, sans distinction et de manière générale, sans suspicion criminelle préalable »[106].

Nous en retrouvons plusieurs usages dans le monde. La surveillance de masse peut être employée comme outil de contrôle et de répression, comme dans le cas du système chinois de crédit social[107]. Elle peut également être utilisée pour atteindre des objectifs politiques, comme la répression des opposants lors des manifestations de Hong Kong, où la reconnaissance faciale a été utilisée pour identifier les manifestants. Il convient de souligner que les utilisations de ces technologies biométriques ne se limitent pas aux États autoritaires, on les retrouve également dans les démocraties libérales, par exemple aux États-Unis où la reconnaissance faciale est utilisée dans les quartiers noirs afin de maintenir l'ordre[108].

En outre, il est relativement facile de tomber dans une surveillance biométrique de masse de diverses manières. Tout d'abord, on pourrait utiliser des bases de données qui étaient collectées à l'origine pour une finalité très précise, autorisée et contrôlée, comme par exemple une base de données pour la fiscalité, et associer ces données à d'autres finalités, telle que la prévention d'activités criminelles, sans justification appropriée[109]. Ensuite, il serait également possible d'utiliser des bases de données pour ajouter de nouvelles fonctionnalités à un système existant, par exemple, en étendant l'utilisation des technologies de reconnaissance faciale utilisée pour les contrôles de carte d'identité effectués à l'aéroport, puis potentiellement dans toute la ville[110]. Selon certains, ce serait une stratégie bien élaborée des fournisseurs de la reconnaissance faciale, qui multiplient les usages d'abord dans des contextes « innocents » qui « facilitent la vie » des consommateurs, comme par exemple le déverrouillage d'un téléphone, pour les habituer à ces technologies et rendre progressivement naturel, voire inévitable, l'adoption d'usages plus étendus[111]. Il est donc important, afin de garantir un contrôle sur les usages des bases de données et de prévenir tout risque de détournement de fonction, d'appliquer rigoureusement le « principe de la limitation des finalités »[112]. Cela implique une

[106] F. RAGAZZI *et al*., *op. cit.*, p. 21.
[107] K. WONG et A. DOBSON, « We're just data: Exploring China's social credit system in relation to digital platform ratings cultures in Westernized democracies », *Global Media and China Volume 4, Issue 2*, Sage Publications, Juin 2019, p. 157.
[108] V. RAPOSO, « The use of facial recognition technology by law enforcement in Europe…», *op. cit*., p. 5.
[109] M. SMITH et S. MILLER, *op. cit.,* p. 173.
[110] T. MADIEGA et H. MILDEBRATH, *op. cit.*, p. 9.
[111] C. CASTELLUCCIA et D. LE MÉTAYER, *op. cit.,* p. 10.
[112] Commission européenne, « Peut-on traiter les données pour toutes les finalités ? », disponible sur https://commission.europa.eu/, *s.d*., consulté le 20 mars 2023. ; Voir *infra*, titre 2.

réglementation stricte concernant le type de données (données criminelles ou civiles, données issues des réseaux sociaux) qui peut être utilisé pour des recherches biométriques[113].

La technologie de reconnaissance faciale à distance et en temps réel peut également entraîner de graves conséquences quant aux attentes de la population en matière d'anonymat dans les espaces publics[114]. En effet, de nos jours, la plupart des individus ont des attentes subjectives en matière de respect de leur vie privée lorsqu'ils se trouvent en public. Bien que des inconnus dans la rue puissent nous regarder et nous dévisager, il est peu probable qu'ils puissent nous identifier par notre prénom, nom, adresse, statut d'immigrant, notre casier judiciaire ou d'autres informations personnelles. Nous nous attendons à pouvoir nous rendre à des endroits « sensibles », tels que chez le médecin ou le psychothérapeute pour des consultations, à la pharmacie, ou dans une clinique afin de procéder à un avortement, sans être reconnus ou obligés de révéler notre identité en public[115]. En fonction de la mesure dans laquelle les technologies de reconnaissance faciale sont utilisées, l'impact sur les personnes peut être si significatif qu'il peut entraver leur droit à mener une vie digne[116]. En effet, n'importe qui peut être considéré comme un suspect, et même des comportements anodins tels que le port de lunettes de soleils ou le fait de regarder le sol peuvent devenir suspects. C'est la raison pour laquelle l'Union européenne a rejeté à plusieurs reprises les intrusions dans la vie privée qui sont considérées comme étant de la surveillance de masse, ou qui pourraient le devenir[117].

Une association européenne de défense des droits et libertés en ligne, dite « EDRI »[118], a ainsi résumé les risques qu'engendrerait la surveillance de masse :

« Une mesure permettant une surveillance constante et en temps réel, impliquant notamment le traitement de données sensibles et de catégorie spéciale telles que les données biométriques faciales, de manière générale ou indiscriminée, violerait en soi l'essence des droits fondamentaux tels que la vie privée, la dignité, la liberté d'expression et la liberté d'association, et serait donc incompatible avec le droit communautaire. »[119].

---

[113] F. RAGAZZI *et al*., *op. cit.*, p. 13.
[114] C. FONTES et C. PERRONE, *op. cit*., p. 5.
[115] M. HIROSE, « Privacy in Public Spaces: The Reasonable Expectation of Privacy Against the Dragnet Use of Facial Recognition Technology », *Connecticut Law Review*, Vol. 49, 2017, p. 1600.
[116] FRA, *op. cit*., p. 20.
[117] V. RAPOSO, « The use of facial recognition technology by law enforcement in Europe… », *op. cit.*, p. 5.
[118] European Digital Rights.
[119] Traduction libre de EDRI, « Ban Biometric Mass Surveillance. A set of fundamental rights demands for the European Commission and EU Member States », disponible sur https://edri.org, 13 mai 2020, p. 21.

Tous ces dangers ont mené Woodrow Hartzog, professeur de droit à l'université de Samford aux États-Unis, à qualifier la technologie de reconnaissance faciale de « mécanisme de surveillance le plus dangereux qui ait été inventé »[120]. Selon lui, sa nature « invisible, ubiquitaire et opaque », ainsi que la grande quantité de photographies déjà disponible dans diverses bases de données, contribuent à créer un sentiment de surveillance généralisée qui justifie son interdiction absolue[121]. L'EDRI adopte la même position sur la question. En effet, pour l'association, le « traitement biométrique est si intrinsèquement intrusif et son fonctionnement si propice à la surveillance de masse qu'il doit être spécifiquement et indéfiniment interdit »[122].

Vera Lúcia Raposo, une autre professeure de droit au Portugal, considère quant à elle que l'objectif ultime est d'autoriser l'utilisation de la technologie de reconnaissance faciale mais sous certaines conditions tout en protégeant les droits fondamentaux des individus et en fournissant les outils nécessaires aux autorités chargées de l'application de la loi pour lutter contre les crimes graves. En effet, la professeure, au lieu de prôner l'interdiction de la technologie biométrique, préconise la création d'un cadre juridique clair et précis au sein de l'Union européenne qui aborderait les questions urgentes en rapport avec l'utilisation de la reconnaissance faciale dans le cadre du maintien de l'ordre public[123].

L'Organe de contrôle belge partage cet avis. En effet, ce dernier estime qu'il doit être possible d'identifier les auteurs d'infractions graves et les victimes par le biais des technologies de reconnaissance faciale en Belgique. Selon lui, il faut se mettre en quête d'outils permettant d'obtenir de meilleurs résultats en établissant notamment une législation claire et en mettant en place des contrôles requis, tout en respectant les limites de la procédure pénale belge[124].

---

[120] Traduction libre de W. HARTZOG, « Facial recognition is the perfect tool for oppression », disponible sur http://cyberlaw.stanford.edu, 2 août 2018. ; C. CASTELLUCCIA et D. LE MÉTAYER, *op. cit.*, p. 8 et 9.
[121] C. CASTELLUCCIA et D. LE MÉTAYER, *op. cit.*, p. 16.
[122] Traduction libre de EDRI, *op. cit.*, p. 22.
[123] V. RAPOSO, « The use of facial recognition technology by law enforcement in Europe… », *op. cit.*, p. 1.
[124] Avis de l'Organe de contrôle de l'information policière relatif à une proposition de résolution 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 1349/001) du 16 juin 2020, p. 27 et 28.

TITRE 2. CADRE JURIDIQUE DE LA RECONNAISSANCE FACIALE

L'impact de l'utilisation de la reconnaissance faciale sur les droits fondamentaux est désormais bien établi. Bien que de nombreux discours continuent à vanter les avantages de ces nouvelles technologies, de nombreuses études démontrent qu'elles ne sont pas aussi neutres qu'on ne le pense[125]. Il est donc crucial, afin d'éviter les dérives et de contrôler ce qui peut être fait ou non, de disposer d'un cadre juridique contraignant. Que ce soit en Belgique ou au sein de l'Union européenne, le développement des technologies de reconnaissance faciale ne se fait pas dans « un total vide juridique »[126] comme nous pourrions le croire au premier abord. Il est encadré par de nombreuses normes de divers niveaux, allant des droits et libertés fondamentaux aux législations nationales.

Nous entamerons ce titre par le développement des règles juridiques actuellement en vigueur au niveau européen (chapitre 1). Nous procéderons ensuite à l'analyse de la proposition de loi européenne relative à l'intelligence artificielle qui vise à harmoniser les règles des États membres (chapitre 2). Enfin, nous examinerons les règles applicables à l'utilisation de la reconnaissance faciale en droit belge (chapitre 3).

CHAPITRE 1. UN LABYRINTHE LÉGISLATIF : LA RECONNAISSANCE FACIALE ET L'UNION EUROPÉENNE

Actuellement, la législation européenne ne prévoit pas de règles spécifiques concernant l'utilisation de la technologie de reconnaissance faciale. Toutefois, il existe plusieurs normes en vigueur, réparties sur plusieurs niveaux de l'ordre juridique de l'Union européenne[127], qui peuvent être appliquées et qui imposent des obligations et des responsabilités, notamment en ce qui concerne la vie privée et la protection des données personnelles[128].

Plus précisément, la Charte des droits fondamentaux de l'Union européenne (ci-après la « Charte ») comprend un ensemble de garanties de base, telles que la protection des données et le respect de la vie privée, qui sont inscrites dans le droit primaire en tant que droits fondamentaux[129]. Ainsi, elle prévoit en son article 52 que toute limitation aux droits consacrés

[125] Y. MENECEUR, « Droits de l'homme, numérique et intelligence artificielle – La perspective du Conseil de l'Europe », *Un droit de l'intelligence artificielle : entre règles sectorielles et régime général*, 1ère édition, Bruxelles, Bruylant, 2023, p. 135.
[126] H. ISAAC (dir.), « Reconnaissance faciale : porter les valeurs de l'Europe », *Renaissance numérique*, juin 2020, p. 41.
[127] T. MADIEGA et H. MILDEBRATH, *op. cit.,* p. 12.
[128] V. RAPOSO, « (Do not) remember my face: uses of facial recognition technology in light of the general data protection regulation », *Information & Communications Technology Law*, Vol. 23, 2023, p. 46.
[129] T. MADIEGA et H. MILDEBRATH, *op. cit.,* p. 12.

par la Charte doit être prévue par la loi, doit être nécessaire, doit répondre véritablement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui et doit respecter l'étendue des droits et libertés[130]. En cas de mise en place d'une technologie de reconnaissance faciale, si celle-ci risque de porter atteinte à un droit fondamental et que cette restriction ne satisfait pas à l'une des conditions établies, l'utilisation de cette technologie pourrait être considérée comme allant à l'encontre de la Charte[131].

Le droit dérivé est responsable de la mise en application des droits fondamentaux et des réglementations sectorielles en matière des technologies émergentes, en détaillant leur élaboration et leur déploiement. Dans ce contexte hiérarchisé, les normes du droit dérivé et leur mise en œuvre doivent être conformes au droit primaire pour assurer la cohérence de l'ensemble du cadre réglementaire[132]. Parmi les normes du droit dérivé, on peut citer le RGPD et la directive (UE) 2016/680 relative à la protection des données dans le domaine répressif[133] (ci-après la « directive police-justice »).

Section 1. À la croisée des règlements

Le RGPD et la directive police-justice composent le « paquet européen de protection des données personnelles »[134]. Ces deux réglementations s'appliquent aux traitements des données biométriques[135] mais possèdent des champs d'application distincts qui se complètent mutuellement. La directive police-justice tout d'abord, est une *lex specialis* et n'est applicable qu'aux traitements des données à caractère personnel par les autorités publiques à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites ou d'exécution des sanctions pénales[136]. Le RGPD quant à lui, s'applique à l'ensemble des traitements de données à caractère personnel dans les États membres, à l'exception toutefois des traitements mis en œuvre pour l'exercice d'activités qui ne relèvent pas du champ d'application du droit de l'Union européenne, et ceux mis en œuvre aux fins de la directive police-justice[137].

---

[130] Art. 52/1 Ch. dr. fond. UE.
[131] H. ISAAC (dir.), *op. cit*., p. 49.
[132] T. MADIEGA et H. MILDEBRATH, *op. cit.,* p. 12.
[133] Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, *J.O.U.E.*, L 119/89, 27 avril 2016 (ci-après abrégé « directive (UE) 2016/680 »).
[134] CNIL, « Le cadre européen », disponible sur www.cnil.fr. *s.d*., consulté le 12 juillet 2023.
[135] Art. 2.1 du R.G.P.D. et art. 2 de la directive (UE) 2016/680.
[136] Considérant 19 du R.G.P.D.
[137] Art. 2.1 du R.G.P.D.

Conformément à l'article 5 du RGPD et à l'article 4 de la directive police-justice, le traitement des images faciales doit répondre à trois conditions essentielles[138]. Premièrement, il doit être licite, loyal et transparent (§1). Deuxièmement, il doit suivre une finalité déterminée, explicite et légitime (§2). Troisièmement, il doit être conforme aux exigences de minimisation des données, d'exactitude des données, de limitation de conservation, de sécurité des données et de responsabilité (§3). À cela s'ajoute une condition qui n'est pas énoncée textuellement dans le RPGD, mais qui est formulée tant dans la jurisprudence[139], que dans la directive-police[140] : le respect du principe de la nécessité et de la proportionnalité (§4).

§1. Traitement licite, loyal et transparent

a) Principe de licéité

Pour être licite, le traitement des données à caractère personnel doit reposer sur des bases juridiques spécifiques[141]. Étant donné que les technologies de reconnaissance faciale traitent généralement des données qui sont liées à des caractéristiques physiques, physiologiques ou comportementales, leur utilisation doit être considérée comme un traitement de données biométriques au sens de l'article 4, paragraphe 14, du RGPD et l'article 3, paragraphe 13, de la directive police-justice[142]. Ce faisant, un tel traitement devra satisfaire aux strictes exigences de l'article 9 du RGPD et l'article 10 de la directive police-justice.

Selon le RGPD, « le traitement des données génétiques, le traitement de données biométriques aux fins d'identifier une personne physique de manière unique [...] sont interdits »[143]. Cette interdiction générale est toutefois assortie d'une dizaine d'exceptions, énumérées de manière exhaustive à l'article 9 en son deuxième paragraphe.

Une des hypothèses dans laquelle le traitement d'une catégorie aussi sensible de données à caractère personnel peut être licite est celle où la personne concernée y a donné son « consentement explicite pour une ou plusieurs finalités spécifiques »[144]. Le texte du Règlement définit et explicite la notion de consentement à plusieurs reprises, en précisant que celui-ci doit

[138] T. MADIEGA et H. MILDEBRATH, *op. cit.,* p. 13.
[139] Cour eur. D.H. (Gde ch.), *S. et Marper c. Royaume-Uni*, 4 décembre 2008, req. n° 30562/04 et 30566/04, §18. ; C.J.U.E. (Gde ch.), 9 novembre 2010, *Volker und Markus Schecke et Eifert*, aff. jointes C-92/09 et C-93/09 ; C. DE TERWANGNE, *op. cit*., p. 20.
[140] Art. 4, §2, b) de la directive (UE) 2016/680.
[141] Considérant 40 du R.G.P.D. et considérant 35 de la directive (UE) 2016/680.
[142] Art. 4.14 du R.G.P.D. et art. 3, §13 de la directive (UE) 2016/680; T. MADIEGA et H. MILDEBRATH, *op. cit.,* p. 13.
[143] Art. 9.1 du R.G.P.D.
[144] Art. 9.2, a) du R.G.P.D.

être donné librement[145], en toute connaissance de cause[146] et sans ambiguïté[147]. Le considérant 43 prévoit une dérogation pertinente : il indique que le consentement sera présumé ne pas avoir été donné librement « en cas de déséquilibre manifeste entre la personne concernée et le responsable du traitement »[148]. Bien que la disposition manque de précision, elle semble suggérer que le consentement donné par un citoyen ordinaire à une autorité publique ne peut être considéré comme une base juridique valable pour le traitement des données du citoyen, étant donné la relation de pouvoir déséquilibrée entre les parties impliquées[149].

À ce sujet, le tribunal administratif de Marseille a rendu le 27 février 2020[150] une décision concernant le déploiement de la technologie de reconnaissance faciale en France. En l'espèce, le conseil régional de Provence-Alpes-Côte d'Azur avait déployé un dispositif de contrôle d'accès virtuel dans deux lycées, consistant en l'installation de portiques de reconnaissance faciale à l'entrée de ces établissements. La région avait affirmé que le traitement de données biométriques était justifié légalement par le consentement préalable des élèves concernés[151]. Le tribunal a fait droit à la requête visant à annuler la décision, en notant spécifiquement qu'« alors que le public visé se trouve dans une relation d'autorité à l'égard des responsables des établissements publics d'enseignement concernés, la région ne justifie pas avoir prévu des garanties suffisantes afin d'obtenir des lycées ou de leurs représentants légaux qu'ils donnent leur consentement à la collecte de leurs données personnelles de manière libre et éclairée »[152].

Une autre hypothèse dans laquelle le traitement des données biométriques peut être licite est lorsque « le traitement est nécessaire pour des motifs d'intérêt public important sur la base du droit de l'Union ou du droit des États membres »[153]. Cette exception pourrait jouer un rôle important notamment lorsque la reconnaissance faciale est déployée à des fins de contrôle d'accès par une autorité publique qui ne souhaite pas s'appuyer sur un consentement explicite ou qui, en raison d'un déséquilibre manifeste entre le responsable de traitement et l'individu concerné, ne remplit pas les conditions d'un « consentement explicite »[154].

---

[145] Art. 7 du R.G.P.D.
[146] Considérant 42 du R.G.P.D.
[147] Considérant 33 du R.G.P.D.
[148] Considérant 43 du R.G.P.D.
[149] T. CHRISTAKIS, K. BANNELIER, C. CASTELLUCCIA, *et al*., « Mapping the Use of Facial Recognition in Public Spaces in Europe – Part 3: Facial Recognition for Authorisation Purposes », *Report of the AI- Regulation Chair - MIAI*, mai 2022, p. 10.
[150] Trib. administratif de Marseille, 27 février 2020, n°1901249, disponible sur www.doctrine.fr.
[151] H. ISAAC (dir.), *op. cit*., p. 56.
[152] Trib. administratif de Marseille, 27 février 2020, n°1901249, point 12, disponible sur www.doctrine.fr.
[153] Art. 9.2, g) du R.G.P.D.
[154] T. CHRISTAKIS, K. BANNELIER, C. CASTELLUCCIA, *et al*., *op. cit*., p. 15.

Concernant cette dernière hypothèse, la Cour d'appel de Barcelone a jugé que l'entreprise de distribution alimentaire « Mercadona » n'était pas autorisée à utiliser un système de reconnaissance faciale pour empêcher deux voleurs condamnés à entrer dans ses supermarchés. La Cour a considéré que cette pratique porterait atteinte aux garanties nécessaires pour protéger les droits et libertés, non seulement des délinquants dont l'accès est interdit, mais également des autres personnes fréquentant le supermarché. Selon la Cour, l'utilisation de la reconnaissance faciale dans ce contexte n'était pas justifiée par un intérêt public, mais plutôt par les intérêts privés de l'entreprise. La décision a par ailleurs été renforcée par l'absence de législation spécifique en Espagne autorisant explicitement l'utilisation d'un système de reconnaissance faciale dans cette situation, ce qui a conduit à l'interdiction de cette pratique[155].

Pour ce qui est des services répressifs, ces derniers doivent respecter des conditions similaires à ceux du Règlement pour pouvoir déployer la reconnaissance faciale, conformément aux articles 4 et 10 de la directive police-justice[156]. Dans le cadre de leurs activités, les services de police utilisent généralement des lois et des réglementations policières en matière de surveillance pour justifier leur utilisation des technologies de reconnaissance faciale, telle que la loi sur la fonction de police en Belgique, qui peut servir de base juridique[157].

En effet, les services de police belges ont déjà essayé d'invoquer cette loi pour justifier la mise en place de caméras de surveillance avec la technologie de reconnaissance faciale à l'aéroport de Zaventem pour une période de test[158]. Cependant, l'Organe de contrôle a considéré que la loi sur la fonction de police était difficilement applicable car la phase de test n'avait pas comme objectif la recherche ou la poursuite d'un délit, et que par ailleurs cette loi ne prévoit pas de base légale spécifique et claire pour l'usage de telles technologies[159].

---

[155] Audiencia Provincial de Barcelona, Sección 9ª, Auto 72/2021 de 15 Feb. 2021, Rec. 840/2021, disponible sur https://diariolaley.laleynext.es/content/Documento.aspx?params=H4sIAAAAAAAAEAMtMSbH1CjUwMDCzNDUwtzRVK0stKs7Mz7Mty0xPzStJBfEz0ypd8pNDKgtSbdMSc4pT1RKTivNzSktSQ4sybUOKSlMBe81L1EUAAAA=WKE.

[156] Art. 4.1, a) du R.G.P.D. et art. 10 de la directive (UE) 2016/680.

[157] T. MADIEGA et H. MILDEBRATH, *op. cit.,* p. 14.

[158] Voir *infra*.

[159] Voy. rapport intermédiaire avec mesure correctrice concernant la visite menée auprès de la police fédérale de l'aéroport de Zaventem par l'Organe de contrôle de l'information policière et portant sur l'utilisation de la reconnaissance faciale (DIO19004), disponible sur www.organedecontrole.be/publications/rapports.

b) Principe de loyauté et transparence

Dans le contexte des technologies de reconnaissance faciale, il est essentiel de fournir des informations claires et transparentes étant donné que les images faciales des individus sont généralement capturées sans leur consentement dans des lieux publics[160]. Le RGPD et la directive police-justice prévoient des dispositions pour assurer la transparence et le droit à l'information[161]. Selon l'article 5 du RGPD, le droit à la protection des données personnelles nécessite un traitement loyal, ce qui signifie que les personnes dont les images faciales sont capturées doivent être informées de manière adéquate[162].

En outre, le RGPD consacre en ses articles 12 à 14 des obligations spécifiques pesant sur le responsable de traitement telles que la communication des coordonnées du responsable du traitement, de la finalité du traitement des données, des délais de conservation, du droit à l'accès aux données stockées et leur effacement ou leur rectification[163]. La fourniture d'informations ne se limite pas à une obligation de transparence en vertu des réglementations européennes concernant la protection des données, elle contribue également à respecter la dignité de l'individu[164].

En pratique, il est souvent très complexe de respecter cette obligation de transparence. L'Organe de contrôle de l'information policière constate notamment dans l'un de ses avis, que les agents de terrain de la police ne sont souvent pas capables d'expliquer le fonctionnement des technologies qu'ils utilisent, voire ne le comprennent pas eux-mêmes. Selon l'Organe, ce problème ne fera que s'aggraver avec l'introduction de systèmes de reconnaissance faciale complexes, étant donné que c'est déjà le cas pour les traitements « ordinaires » de simples caméras[165]. De plus, comme nous l'avons souligné précédemment, la majorité des systèmes de surveillance demeurent opaques. Il existe peu d'informations sur la manière dont les données des individus sont traitées lorsqu'ils entrent dans des espaces publics sous surveillance. Il est rare qu'ils se voient offrir des alternatives concrètes s'ils ne souhaitent pas être soumis à une surveillance[166].

---

[160] FRA, *op. cit*., p. 24.
[161] Art. 5, §1er, a), R.G.P.D. et considérant 26 de la directive (UE) 2016/680.
[162] FRA, *op. cit.*, p. 24.
[163] Art. 12 à 14 du R.G.P.D. ; FRA, *op. cit*., p. 24.
[164] FRA, *op. cit*., p. 24.
[165] Avis de l'Organe de contrôle de l'information policière relatif à une proposition de résolution 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 ou privés, disponible sur https://www.organedecontrole.be/files/DA210029_Avis_F.pdf., p. 23.
[166] F. RAGAZZI *et al*., *op. cit*., p. 12.

Ce constat nous conduit à affirmer qu'il est nécessaire d'étendre les exigences de transparence et de responsabilité. Certains auteurs, dont Yves Poullet, pointent également du doigt le fait que les obligations découlant des articles 12 à 14 du RGPD se limitent uniquement au responsable du traitement et au sous-traitant alors qu'il est important d'imposer certains devoirs aux fournisseurs des composants d'une application de reconnaissance faciale[167]. Cela nous amène à considérer que le RGPD présente certaines lacunes et pourrait ne pas être l'outil le mieux adapté pour relever les « défis de l'intelligence artificielle »[168].

§2. Finalité déterminée, explicite et légitime

« Véritable pierre angulaire de la protection des données »[169], le principe de la limitation des finalités est consacré non seulement à l'article 5 du RGPD et à l'article 4 de la directive police-justice, mais aussi au deuxième paragraphe de l'article 8 de la Charte[170]. Ce principe exige que les données ne soient collectées que pour des finalités déterminées, explicites et légitimes, et que toute utilisation ultérieure des données pour une finalité différente, ne peut être autorisée que sous certaines conditions[171]. Cela signifie également que la finalité doit être formulée de manière claire et précise, de sorte que la personne concernée soit en mesure d'anticiper la finalité pour laquelle ses données seront traitées[172].

Dans le contexte du traitement des données au moyen des technologies de reconnaissance faciale, il est important que la finalité du traitement des images faciales soit strictement déterminée, et qu'elle se limite principalement, dans le cadre des activités répressives, à la lutte contre les crimes graves. En outre, ces technologies pourraient être utilisées pour identifier les personnes disparues et les victimes de criminalité, y compris les enfants[173].

§3. Principe de minimisation des données

Selon l'article 5, paragraphe 1, point c) du Règlement et l'article 4, paragraphe 1, point c) de la directive police-justice, le principe de minimisation est interprété comme exigeant que

---

[167] Y. POULLET, *op. cit*., p. 133.
[168] Y. POULLET, *ibidem.*
[169] C. DE TERWANGNE, *op. cit.*, p. 22.
[170] Art. 8, §2, Ch. dr. fond. UE ; art. 5.1 du R.G.P.D. et art. 4, §1er, b) de la directive (UE) 2016/680.
[171] T. MADIEGA et H. MILDEBRATH, *op. cit.,* p. 17.
[172] T. MADIEGA et H. MILDEBRATH, *ibidem,* p. 17. ; FRA, op. cit., p. 25. ; CJEU, C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU*, Conclusions de l'avocat général Kokott, J., 18 juillet 2007, point 53.
[173] FRA, *op. cit*., p. 25.

la quantité de données soit limitée à ce qui est strictement nécessaire par rapport aux objectifs du traitement[174]. Ce principe implique que l'on ne traite des données personnelles que lorsque cela est raisonnablement nécessaire pour atteindre l'objectif visé. Le considérant 39 précise également que cela implique que la durée de conservation des données soit limitée au strict minimum[175].

Ainsi, l'Autorité française de protection des données, par exemple, a conclu que le déploiement d'un système de contrôle d'accès basé sur la reconnaissance faciale dans les établissements scolaires constituait une violation des principes de proportionnalité et de minimisation des données. En effet, l'Autorité a considéré que les objectifs de réduction de la durée des contrôles et de sécurisation de l'entrée auraient pu être atteints par des moyens moins intrusifs, tels qu'un système de badge[176].

§4. Principe de nécessité et proportionnalité

Le fait d'avoir obtenu un consentement explicite ou d'avoir eu la possibilité de se prévaloir d'un des motifs d'intérêt public important, ne libère pas le responsable de traitement des données de sa responsabilité de prouver que le traitement des données est nécessaire et proportionné[177]. En effet, selon la recommandation de l'Autorité de protection des données relative au traitement des données biométriques, « le test obligatoire de proportionnalité s'inscrit dans le respect des obligations imposées par le RGPD. Ce n'est que lorsque le responsable du traitement peut efficacement démontrer que tous les principes de la protection des données ont été respectés que l'on peut parler d'un traitement de données licite et donc proportionné »[178]. Autrement dit, même si les personnes concernées ont donné leur consentement pour la collecte de leurs données par le biais de la reconnaissance faciale, le traitement de données pourrait être jugé illégal par un juge ou une autorité de contrôle s'il ne respecte pas l'exigence de proportionnalité[179].

L'Autorité de protection des données poursuit en indiquant que le responsable du traitement des données doit prendre en compte les intérêts importants en jeu ainsi que les risques

---

[174] Art. 5.1, c) du R.G.P.D.; art. 4., §1er, c) de la directive (UE) 2016/680 ; T. MADIEGA et H. MILDEBRATH, *op. cit.,* p. 18.
[175] C. DE TERWANGNE, *op. cit.*, p. 23.
[176] CNIL, « Expérimentation de la reconnaissance faciale dans deux lycées : la CNIL précise sa position », disponible sur www.cnil.fr, 29 octobre 2019.
[177] T. CHRISTAKIS, K. BANNELIER, C. CASTELLUCCIA, *et al*., *op. cit*., p. 19.
[178] Autorité de protection des données, « Recommandation relative au traitement de données biométriques... », *op. cit*., p. 31.
[179] C. DE TERWANGNE, *op. cit.*, p. 21.

pour les droits et libertés des personnes concernées. Pour évaluer cette balance, il est recommandé de considérer la manière dont le traitement proposé affecte la société, à la fois « en profondeur » en évaluant l'impact global du traitement sur les bénéfices ou les préjudices, et « en largeur » en considérant « le nombre de personnes qui perçoivent un avantage ou un préjudice »[180]. Pour illustrer ses propos, l'Autorité de contrôle prend l'exemple de l'utilisation de l'authentification biométrique pour contrôler l'accès aux locaux d'une centrale nucléaire. Dans ce cas-là, les avantages liés à la sécurité de l'infrastructure critique pour l'ensemble de la population l'emportent sur le préjudice perçu par un groupe relativement restreint d'employés concernés par l'utilisation de la technologie biométrique[181].

Section 2. Disparités entre États membres

Comme nous pouvons le constater, la législation européenne impose des exigences strictes aux différents États membres afin de garantir la protection de la vie privée et des données[182] et assurer la légalité de l'application de la reconnaissance faciale[183]. Margrethe Vestager, vice-présidente de la Commission européenne chargée des affaires numériques, considère qu'en l'état actuel des choses, le RGPD indique qu'il ne faut pas utiliser les technologies de reconnaissance faciale car il est relativement difficile, voire impossible, d'obtenir le consentement clair et sans réserve des personnes concernées. Elle critique donc cette méthode qui enfreint les dispositions du Règlement[184]. Toutefois, elle précise qu'il existe certaines exceptions à cette règle, notamment pour des raisons de sécurité publique et invite de surcroit les autorités nationales responsables des données à examiner « les fondements juridiques qui permettront aux États membres de prendre leurs propres décisions au niveau national »[185].

Dans ce contexte, les États membres ont adopté des approches différentes en matière d'application du cadre juridique européen pour le traitement des données biométriques. En effet, le RGPD et la directive police-justice ne cherchent pas à harmoniser les règles applicables au traitement des données biométriques mais plutôt à donner une certaine marge de manœuvre

[180] Autorité de protection des données, « Recommandation relative au traitement de données biométriques... », *op. cit.,* p. 31.
[181] Autorité de protection des données, *ibidem,* p. 31.
[182] T. MADIEGA et H. MILDEBRATH, *op. cit.,* p. 26 et 27.
[183] K. KONSTANTINOS, « Facial recognition: A Challenge for Europe or a Threat to Human Rights? », *Eur. J. Privacy L. & Tech*., 2021, p. 148.
[184] J. VALERO, « Margrethe Vestager s'alarme des dérives de la reconnaissance faciale », disponible sur www.euroactiv.fr, 17 février 2020.
[185] K. KONSTANTINOS, *op. cit.*, p. 148.

aux États membres[186]. Cela est particulièrement visible au dernier paragraphe de l'article 9 qui prévoit que « les États membres peuvent maintenir ou introduire des conditions supplémentaires, y compris des limitations, en ce qui concerne le traitement des données biométriques [...] »[187]. La France a par exemple adopté un article 44 dans sa loi relative à l'informatique et aux fichiers, qui prévoit des exceptions à l'interdiction générale de traitement des données biométriques[188]. Selon cet article, les traitements biométriques nécessaires à la recherche publique sont autorisés, pour autant que des motifs d'intérêt public important les rendent nécessaires[189]. Contrairement à la France, la Belgique n'a pas prévu de telle exceptions[190].

Afin de niveler ces disparités d'application des systèmes d'intelligence artificielle entre États, il est prévu d'adopter une loi européenne spécifique. Cette dernière viendrait harmoniser les diverses règles concernant l'intelligence artificielle et créerait le tout premier cadre juridique pour l'intelligence artificielle, non seulement en Europe, mais également dans le reste du monde[191].

CHAPITRE 2. VERS UNE RÉGLEMENTATION EUROPÉEENNE DE LA RECONNAISSANCE FACIALE – L' « *AI ACT* »

Section 1. Contexte et objectifs

La Commission européenne a publié, le 21 avril 2021, une proposition de loi visant à harmoniser les règles relatives à l'intelligence artificielle et à la reconnaissance faciale[192] (en abrégé l'« *Artificial Intelligence Act* » ou l'« *AI Act* ») et qui est toujours en cours de négociation au moment de la rédaction de ce mémoire. Les institutions européennes avaient préparé le terrain en amont en produisant des documents basés sur une approche humaniste en ce qui concerne l'intelligence artificielle, tels que les « Lignes directrices en matière d'éthique pour une IA digne de confiance » publiées par le groupe d'experts de haut niveau sur

[186] H. ISAAC (dir.), *op. cit*., p. 69.
[187] Art. 9.4 du R.G.P.D.
[188] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifié par l'Ordonnance n°2018-1125 du 12 décembre 2018 (ci-après abrégée « Loi Informatique et Libertés »), art. 44, 6°.
[189] H. ISAAC (dir.), *op. cit*., p. 69. ; Loi Informatique et Libertés précitée, art. 44.
[190] Autorité de protection des données, « Recommandation relative au traitement de données biométriques... », *op. cit*., p. 26.
[191] A. KRACHLER, *op. cit.*, p. 500.
[192] Proposition de règlement (UE) 2021/0106 du Parlement européen et du Conseil du 24 avril 2021 précitée. Pour une analyse approfondie de la proposition, lire le rapport détaillé de N. SMUHA, E. AHMED-RENGERS, A. HERKENS *et al.,* « How the EU can achieve Legally Trustworthy AI : A response to the European Commission's proposal for an Artificial intelligence Act », *University of Birmingham Leads Lab report*, disponible sur https://papers.ssrn.com, 5 août 2021.

l'intelligence artificielle en avril 2019, et le Livre blanc sur l'IA publié en 2021 par la Commission européenne[193]. La proposition d'harmonisation répond aux demandes du Parlement et du Conseil européens qui visent à prendre des mesures garantissant le bon fonctionnement du marché de l'intelligence artificielle, en évaluant attentivement les avantages et les risques qui y sont associés. Ce projet repose notamment sur les inquiétudes suscitées par l'imprévisibilité, le manque de transparence, l'autonomie de certains systèmes d'intelligence artificielle, ainsi que les dangers liés aux erreurs et aux biais. Il a une valeur juridique relativement solide car il vise à établir un ensemble de règles contraignantes pour le développement et l'utilisation des différentes technologies en Europe[194].

La Commission a estimé qu'une intervention au niveau de l'Union européenne était nécessaire pour éviter que les États membres, chacun avec sa propre approche, génèrent une insécurité juridique et n'entravent l'adoption des nouvelles technologies sur le marché européen. De plus, seul un cadre réglementaire commun de l'intelligence artificielle peut assurer des conditions de concurrence équitables entre les entreprises, renforcer la compétitivité des États membres et protéger la souveraineté numérique de l'Europe[195].

En établissant de nouvelles normes, Margrethe Vestager vise à « ouvrir la voie à une technologie éthique dans le monde entier, tout en préservant la compétitivité de l'UE. À l'épreuve du temps et propices à l'innovation, nos règles s'appliqueront lorsque c'est strictement nécessaire: quand la sécurité et les droits fondamentaux des citoyens de l'Union sont en jeu »[196].

Section 2. Contrôle par la gestion des risques

En examinant la proposition de loi sur l'intelligence artificielle de l'UE, nous pouvons constater qu'elle établit ses règles en fonction de trois catégories de risques potentiels que l'utilisation de l'intelligence artificielle (désignée ci-après l'« IA ») peut engendrer : un risque minime ou limité, dont l'utilisation est autorisée avec peu ou sans restrictions[197], (i) un risque

[193] G. MOBILIO, « Your face is not new to me – Regulating the surveillance power of facial recognition technologies », *Internet Policy Review*, 2023, p. 18.
[194] A. MARTIN, « L'intelligence artificielle peut-elle être saisie par le droit de l'Union européenne ? », *Conférence Nationale en Intelligence Artificielle*, disponible sur http://hal.science, 2022.
[195] A. MARTIN, *ibidem.*
[196] Commission européenne, « Une Europe adaptée à l'ère du numérique : La Commission propose de nouvelles règles et actions en faveur de l'excellence et de la confiance dans l'intelligence artificielle », disponible sur https://ec.europa.eu, 21 avril 2021.
[197] Nous ne traiterons pas du risque minime et du risque limité dans le cadre de ce mémoire étant donné que le projet de règlement ne prévoit pas d'intervention dans ce domaine. Toutefois, une précision doit être apportée pour le risque dit limité, qui doit respecter l'obligation de transparence ; Proposition de règlement (UE) 2021/0106 du Parlement européen et du Conseil du 24 avril 2021 précitée, exposé des motifs, p. 8.

considéré comme inacceptable, selon lequel l'utilisation de l'IA est interdite (article 5) et (ii) un système d'IA à haut risque, dont l'utilisation est soumise à certaines conditions, y compris une évaluation préalable de la conformité (article 6)[198].

(i) Le risque inacceptable englobe les systèmes d'IA qui sont perçus comme une menace pour la sécurité. Cela inclut notamment des systèmes d'IA qui « altèrent substantiellement le comportement »[199] humain afin de priver les utilisateurs de leur libre arbitre, tels que des jouets utilisant une assistance vocale pour inciter des mineurs à adopter un comportement dangereux, et des systèmes qui permettent aux États de procéder à une notation sociale de la population[200].

(ii) Le risque élevé concerne quant à lui, les systèmes d'IA qui sont considérés comme étant à « haut risque ». Cette catégorie englobe notamment les technologies d'IA utilisées dans les services essentiels tant privés que publics, les technologies d'IA utilisées dans le domaine de l'emploi et de l'accès à l'emploi indépendant, ainsi que les technologies d'IA utilisées dans le domaine du maintien de l'ordre, qui sont susceptibles d'interférer avec les droits fondamentaux des individus[201]. Les articles 9 à 15 de la proposition établissent des exigences auxquelles les systèmes d'IA à haut risque doivent se conformer pour pouvoir être mis sur le marché[202]. Ces obligations sont mises à charge des fournisseurs, incluant les autorités publiques ou opérateurs privés lorsqu'ils déploient un système sous leur nom ou apportent des modifications aux systèmes, ainsi qu'aux importateurs et aux utilisateurs professionnels[203]. Les sanctions pour les pratiques interdites ou le non-respect des obligations concernant les systèmes d'IA à haut risque sont importantes. Les amendes administratives peuvent atteindre des sommes allant jusqu'à 20 ou même 30 millions d'euros. Il reste à déterminer si ces mesures réglementaires ne vont pas pénaliser les petits fournisseurs d'IA qui n'ont peut-être pas les moyens nécessaires pour se conformer aux exigences[204].

---

[198] F. RAGAZZI *et al*., *op. cit.*, p. 62.
[199] Proposition de règlement (UE) 2021/0106 du Parlement européen et du Conseil du 24 avril 2021 précitée, dispositions générales, art. 5, §1er.
[200] Commission européenne, « Une Europe adaptée à l'ère du numérique... », *op. cit*.
[201] Commission européenne, « Une Europe adaptée à l'ère du numérique... », *ibidem.*
[202] Nous retrouvons notamment l'exigence de transparence et de fourniture d'informations aux utilisateurs (art. 13), un contrôle humain approprié (art. 14), un système adéquat de gestion des risques (art. 9), etc.
[203] Proposition de règlement (UE) 2021/0106 du Parlement européen et du Conseil du 24 avril 2021 précitée, dispositions générales, art. 16 à 29.
[204] A. STROWEL, « L'intelligence artificielle : vers une régulation européenne par la gestion des risques », *Les pages : obligations, contrats et responsabilités*, Vol. 2021, no.99, p. 1.

Section 3. La reconnaissance faciale sous l'AI Act

Les technologies de reconnaissance faciale n'ont pas encore été traitées en détail mais la proposition présente les systèmes d'identification biométrique à distance fondés sur l'IA comme des systèmes à haut risque[205]. Une précision est faite à l'article 5, en son premier paragraphe, point d, qui rappelle que leur utilisation « en temps réel » dans les espaces publics à des fins répressives est interdite. Toutefois, des exceptions existent à ce principe. Elles sont strictement définies et réglementées : la recherche ciblée de victimes potentielles de crimes, la prévention d'une menace terroriste spécifique, substantielle et imminente et la détection, la localisation, l'identification ou la poursuite de l'auteur ou du suspect d'une infraction pénale grave[206]. Dans tels cas, l'utilisation de ces systèmes doit alors être autorisée par une instance judiciaire ou une autorité administrative indépendante[207].

En analysant de plus près les exceptions, nous pouvons relever le fait qu'elles sont toutes rédigées de manière relativement générale, ce qui peut donner l'impression qu'il est aisé de contourner l'interdiction[208]. En effet, pour la première exception, nous pouvons nous demander ce que signifie exactement « la recherche ciblée de victimes potentielles spécifique de la criminalité ». Est-ce que la mise en place de caméras de surveillance à l'aéroport pourrait être considérée comme une recherche ciblée ? Doit-on inclure tous les crimes au-dessus d'un certain seuil, ou cela doit-il être évalué au cas par cas ? En ce qui concerne la deuxième exception liée à la prévention d'une menace terroriste, nous pouvons également nous questionner sur la signification des termes « spécifique, substantielle et imminente ». Ces notions n'étant pas décrites dans la proposition, les États membres pourraient être tentés de les interpréter de manière large lors de la mise en place de lois nationales, ce qui pourrait affaiblir l'interdiction d'identification biométrique à distance. La troisième exception portant sur la détection, la localisation, l'identification, la localisation ou la poursuite d'un suspect d'une infraction pénale qui est passible d'une peine (ou d'une mesure) privative de liberté d'une durée maximale d'au moins trois ans, soulève également des questionnements sur la justification du seuil de trois ans. Est-il suffisamment élevé ou non ? Il est évident que la façon dont ces conditions doivent

[205] D. ALMEIDA, K. SHMARKO et E. LOMAS, « The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU and UK regulatory frameworks », *AI and Ethics*, 2022, p. 381.
[206] Proposition de règlement (UE) 2021/0106 du Parlement européen et du Conseil du 24 avril 2021 précitée, dispositions générales, art. 5, §1er, d).
[207] Proposition de règlement (UE) 2021/0106 du Parlement européen et du Conseil du 24 avril 2021 précitée, dispositions générales, art. 5, §3.
[208] P. STUBBE, « Het gebruik van facial recognition door de Belgische politiediensten », mémoire, Université de Gand, 2021-2022, p. 103.

être interprétées n'est pas totalement claire, ce qui pourrait entrainer des problèmes potentiels[209].

En outre, il mérite d'être souligné que la proposition de loi européenne sur l'IA ne dit rien des autres modalités de la technologie de reconnaissance faciale à des fins répressives, par exemple lorsque cette technologie n'est pas utilisée en temps réel ou dans des espaces publics, ou encore lorsqu'elle est utilisée à d'autres fins que l'identification. De plus, elle n'interdit pas non plus l'utilisation de la reconnaissance faciale pour des objectifs autres que répressifs, ni par des individus ou des entreprises[210]. Toutes ces possibilités doivent donc être considérées comme admissibles.

Section 4. Vers une interdiction absolue ?

Suite à la proposition de la Commission européenne datant de 2021, le Conseil de l'Union européenne a également exprimé sa position sur le projet européen en décembre 2022. Dans cette approche, le Conseil a défini de manière plus précise les objectifs justifiant l'utilisation des systèmes d'identification biométrique en temps réel à des fins répressives dans les espaces publics et a restreint l'autorisation d'utilisation de tels systèmes par les services répressifs à des situations exceptionnelles[211].

Le 14 juin 2023, le Parlement européen a, à son tour, adopté sa position concernant l'élaboration de la réglementation sur l'intelligence artificielle, déclenchant ainsi des discussions et négociations entre les trois géants de l'Union européenne - la Commission européenne, le Conseil et le Parlement, afin de réconcilier les trois versions différentes de l'AI Act[212].

Contrairement aux deux autres institutions européennes, le Parlement a décidé d'interdire toute identification biométrique à distance et en temps réel dans les espaces accessibles au public. L'amendement 41 précise que les systèmes d'identification biométrique à distance et a posteriori sont également interdits, « sauf lorsqu'ils sont strictement nécessaires à la recherche ciblée liée à un crime grave précis déjà commis, et uniquement sous réserve de l'approbation du tribunal »[213].

---

[209] P. STUBBE, *ibidem,* p. 104.
[210] V. RAPOSO, « The use of facial recognition technology by law enforcement in Europe… », *op. cit.*, p. 4.
[211] Council of the European Union, « Artificial Intelligence Act: Council calls for promoting safe AI that respects fundamental rights », disponible sur www.consilium.europa.eu, 6 décembre 2022.
[212] L. BERTUZZI, « Le règlement de l'UE sur l'IA entre dans la phase finale du processus législatif », disponible sur www.euractiv.fr, 15 juin 2023.
[213] Proposition de règlement (UE) 2021/0106 du Parlement européen et du Conseil du 24 avril 2021 précitée, amendements adoptés par le Parlement européen le 14 juin 2023.

Certains, dont des start-up et des grandes entreprises, estiment que le Parlement a adopté une position beaucoup trop radicale et « dangereuse pour l'innovation »[214]. D'autres, telles que la conseillère politique principale à l'EDRI – Ella Jakubowska, considèrent que « c'est le signal le plus clair à ce jour que le Parlement européen a mis en avant la protection de tous nos droits à vivre librement et dignement dans les espaces publics, plutôt que les profits privés et les fausses revendications de 'sécurité' »[215]. En effet, lorsqu'on examine attentivement le RGPD, la directive police-justice et la proposition de législation européenne, aucun de ces textes ne rejette catégoriquement les technologies dont l'utilisation peut être dangereuse et préjudiciable dans des domaines spécifiques à haut risque. Leur refus semble « faux » car il est assorti de nombreuses exceptions qui, en fin de compte, le rendent permissif[216]. Il est possible que ces règlementations n'aient pas voulu freiner l'innovation et qu'elles n'aient pas pleinement appréhendé les enjeux spécifiques liés à la technologie de reconnaissance faciale. Ces instruments juridiques ont probablement eu du mal à détecter les abus potentiels de ces technologies et à les distinguer des autres[217]. En revanche, le Parlement européen, probablement en réponse à de multiples pétitions signées dans plusieurs pays européens s'opposant à l'usage de telles technologies[218], a adopté une approche plus franche et a eu le courage d'interdire sans détour la reconnaissance faciale à distance.

Cette prise de position risque d'être le point de discorde lors de prochaines discussions avec les États membres au sein du Conseil de l'UE car beaucoup souhaitent autoriser les forces de l'ordre à utiliser la reconnaissance faciale en temps réel, comme l'a fait la Commission dans son rapport initial[219]. Il est prévu d'atteindre un compromis final d'ici la fin de l'année afin que la future loi européenne entre en vigueur en 2026[220], mais vu la complexité des enjeux en présence, cela risque d'être un véritable parcours du combattant.

---

[214] A. PIQUARD, « Intelligence artificielle : négociations tendues autour du projet de règlement européen AI Act », disponible sur www.lemonde.fr, 18 juillet 2023.
[215] J. CONLEY, « In 'Win for Fundamental Rights', EU Advances AI Rules Restricting Facial Recognition », disponible sur www.commondreams.org, 14 juin 2023.
[216] P. DE HERT et G. BOUCHAGIAR, « Visual and biometric surveillance in the EU. Saying 'no' to mass surveillance practice? », *Information Polity,* Vol. 27, 2022, p. 211.
[217] P. DE HERT et G. BOUCHAGIAR, *ibidem*, p. 211.
[218] Notamment le mouvement européen 'Reclaim Your Face' qui appelait à signer une pétition contre l'utilisation de la reconnaissance faciale à l'échelle européenne, disponible sur www.reclaimyourface.eu.
[219] V. GEORIS, « Le Parlement européen ne veut pas de la reconnaissance faciale par IA », disponible sur www.lecho.be, 14 juin 2023.
[220] Parlement européen, « Loi sur l'IA de l'UE : première réglementation de l'intelligence artificielle », disponible sur www.europarl.europa.eu, 6 juin 2023.

CHAPITRE 3. RÈGLES APPLICABLES AU NIVEAU NATIONAL

En Belgique, la reconnaissance faciale ne fait pas l'objet d'un encadrement juridique spécifique. Toutefois, certaines législations en vigueur peuvent servir de jalons pour encadrer cette technologie et garantir le respect des droits fondamentaux tout en évitant d'éventuels abus. Plus précisément, trois législations doivent être prises en considération lors de la mise en place des technologies de reconnaissance faciale dans le contexte belge. La première relative à la protection des données (section 1), et la deuxième ainsi que la troisième à la fonction de police et à la vidéosurveillance (section 2). Nous examinerons ensuite la position de l'Autorité de protection des données quant à l'usage de la reconnaissance faciale comme moyen d'authentification et d'identification (section 3). Enfin, nous mettrons en lumière les évolutions potentielles de la réglementation belge concernant la reconnaissance faciale (section 4).

Section 1. La loi relative à la protection des données

Le RGPD a été implémenté en Belgique par la loi « vie privée » du 8 décembre 1992[221], qui a été ensuite abrogée le 5 septembre 2018, date à laquelle est entrée en vigueur la nouvelle loi générale (ci-après « loi-cadre »)[222] qui vient compléter le RGPD sur les aspects laissés à la discrétion des États membres, ainsi que sur les domaines couverts par la directive 2016/680[223].

§1. Traitement des données biométriques

L'article 34 de la loi-cadre retranscrit l'article 9 du RGPD qui pose une interdiction du traitement des données biométriques. Cette interdiction est toutefois accompagnée de trois exceptions. Premièrement, le traitement est autorisé lorsqu'il est prévu par la loi, le décret, l'ordonnance, le droit de l'Union européenne ou l'accord international. Deuxièmement, il est autorisé lorsqu'il est nécessaire à la défense des intérêts vitaux de la personne concernée ou d'une autre personne physique. Enfin, le traitement est permis si les données ont été rendues publiques par la personne concernée[224].

À l'heure actuelle en Belgique, il existe une seule loi qui permet explicitement le traitement des données biométriques à des fins non répressives, à savoir la loi relative aux

[221] Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personne, *M.B.*, 18 mars 1993.
[222] Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, *M.B.*, 5 septembre 2018.
[223] C. DE TERWANGNE, *op. cit.*, p. 9.
[224] Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel précitée, art. 34.

registres de la population, aux cartes d'identité, aux cartes des étrangers et aux documents de séjour[225]. De plus, il existe le règlement européen établissant des normes pour les éléments biométriques intégrés dans les passeports délivrés par les États membres[226]. Cependant, contrairement à certains pays voisins[227], les autorités belges n'ont pas choisi de mettre en place de base légale générale pour autoriser le traitement des données biométriques dans le cadre de l'identification ou de l'authentification unique d'une personne. En conséquence, à l'exception du traitement des données biométriques liés à la carte d'identité électronique et au passeport, il subsiste un vide juridique dans la législation belge qui rend tout autre traitement des données biométriques dépourvu de fondement légal[228].

En ce qui concerne le traitement des données biométriques par les services de police, le législateur belge a choisi de le réglementer dans la loi sur la fonction de police qui sera expliquée plus en détail ultérieurement.

§2. Organe de contrôle de l'information policière

La loi-cadre crée l'Organe de contrôle de l'information policière (ci-après « COC ») et lui confère une mission de surveillance et de contrôle à l'égard de tous les traitements opérationnels et non opérationnels à caractère personnel effectués par la police fédérale ainsi que la police locale[229]. Dans ce cadre, le COC fournit des avis, des constatations, des recommandations ou des avertissements. Compte tenu de l'expertise de l'Organe de Contrôle en matière de protection des données, son avis jouera un rôle crucial dans l'établissement d'un potentiel cadre juridique solide concernant les technologies de reconnaissance faciale à l'avenir. Une autre mission essentielle du COC est d'enquêter sur les affaires liées à ces technologies[230]. Ses membres ont le droit de consulter toutes les informations et les données traitées par les services de police, et lors de ces enquêtes, ils ont un accès illimité aux locaux où ces données et informations ont été traitées et peuvent même saisir des éléments qui leur semblent utiles[231].

---

[225] Loi du 19 juillet 1991 relative aux registres de la population, aux cartes d'identité, aux cartes des étrangers et aux documents de séjour, *M.B*., 3 septembre 1991.
[226] Règlement (CE) n° 2252/2004 du Conseil du 13 décembre 2004 établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres.
[227] Par exemple la France voy. loi Informatique et Libertés, article 6.II.
[228] Autorité de protection des données, « Recommandation relative au traitement des données biométriques... », *op. cit.,* p. 26.
[229] Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel précitée, art. 71, §1er.
[230] Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel précitée, art. 240, 4° et art. 242.
[231] Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel précitée, art. 244, §3.

Suite aux enquêtes, l'Organe de Contrôle prend des décisions concernant les plaintes, et ses pouvoirs lui permettent notamment de recourir à des mesures correctrices qui sont des injonctions contraignantes si des violations aux règlements applicables sont constatées[232].

L'Organe de Contrôle a mené deux enquêtes sur l'utilisation des technologies de reconnaissance faciale par les services de police, une en 2019 et une autre en 2022, publiant des rapports détaillant leurs principales conclusions. Pour une compréhension complète des points de vue de l'Organe de Contrôle, il est nécessaire d'examiner d'abord la loi sur la fonction de police. Les résultats de ces enquêtes seront présentés dans le titre 3.

Section 2. Loi sur la fonction de police et loi caméras

Dans cette section, nous traitons de deux lois réglant l'utilisation des caméras de surveillance: la loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance[233], également connue sous le nom de « loi caméras » et la loi sur la fonction de police du 5 août 1992[234] (ci-après « LFP »). Ces deux textes législatifs ont fait l'objet de plusieurs modifications pertinentes en 2018, lesquelles méritent d'être examinées attentivement.

§1. Modifications législatives

En 2018, une nouvelle loi a été adoptée pour modifier les deux lois relatives à la surveillance afin de répondre aux besoins particuliers des services de police en matière d'utilisation des caméras[235]. Auparavant, la loi caméras était applicable à l'usage de caméras par les services de police dans le cadre de leurs missions de police administrative et judiciaire. Cependant, avec l'évolution de la société basée sur les nouvelles technologies, les services de police avaient besoin de moyens plus sophistiqués pour mener à bien leurs missions, dépassant les dispositions de la loi caméras. Le législateur s'est donc demandé s'il était préférable de modifier la loi caméras en l'adaptant aux besoins des services de police ou de créer de nouvelles règles dans une législation policière. Il a été opté pour la deuxième option : les nouvelles règles

[232] Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel précitée, art. 244 et 247.
[233] Loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance, *M.B*., 31 mai 2007.
[234] Loi du 5 août 1992 sur la fonction de police, *M.B.,* 22 décembre 1992.
[235] Loi du 21 mars 2018 modifiant la loi sur la fonction de police, en vue de régler l'utilisation de caméras par les services de police, et modifiant la loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance, la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et la loi du 2 octobre 2017 réglementant la sécurité privée et particulière, *M.B*., 16 avril 2018.

ont été incluses dans la loi sur la fonction de police qui réglemente les compétences générales des services de police, et ont ainsi exclu l'application de la loi caméras aux caméras des services de police[236].

§2. L'utilisation policière des caméras de surveillance

Nous retrouvons donc dans la LFP de nouvelles règles sur l'utilisation des caméras mobiles et des caméras dites « intelligentes »[237]. Selon les travaux parlementaires, ces dernières sont couplées d'une technologie supplémentaire qui va au-delà du simple traitement d'images, comme par exemple les caméras de reconnaissance faciale ou les caméras de reconnaissance automatique des plaques d'immatriculation (ANPR)[238]. Nous identifions particulièrement l'article 25/3 qui autorise l'utilisation de ces caméras intelligentes en temps réel par les services de police dans l'exercice de leurs fonctions administratives et judiciaires, sous réserve qu'elles soient utilisées en public, dans des lieux fermés librement accessibles au public ou non[239].

En outre, la loi sur la fonction de police établit les pouvoirs des services de police en matière de collecte d'informations et prévoit en son article 44/1 que les données biométriques qui catégorisent différentes personnes, telles que celles ayant enfreint l'ordre public ou faisant l'objet d'une ordonnance de surveillance, « sont traitées uniquement dans le but d'assurer l'identification » de ces personnes[240]. Si ce traitement engendre potentiellement un risque élevé pour les droits et libertés des individus concernés, la police doit consulter l'Organe belge de contrôle de l'information policière[241]. Par conséquent, la loi n'interdit pas le traitement des données biométriques des personnes recherchées par les services de police. De fait, l'article 44/1 de la LFP pourrait même en être le fondement juridique. Dans cette hypothèse, l'Organe de contrôle serait l'autorité compétente pour aider à la mise en place de ce traitement[242].

Toutefois, il convient de souligner que la loi prévoit exclusivement la création d'une « banque de données technique » destinée aux caméras intelligentes de reconnaissance automatique de plaques d'immatriculation, aussi bien au niveau local que national[243], mais elle

---

[236] Projet de loi modifiant la loi sur la fonction de police, en vue de régler l'utilisation de caméras par les services de police, et modifiant la loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance, la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et la loi du 2 octobre 2017 réglementant la sécurité privée et particulière, Exposé des motifs, *Doc*., Ch., 2018, n°2855/001, p. 6 et 7.
[237] Loi du 5 août 1992 sur la fonction de police précitée, art. 25/2, 1° et 3°.
[238] Commentaire des articles précité, *Doc*., Ch., 2018, n°2855/001, p. 11.
[239] Loi du 5 août 1992 sur la fonction de police précitée, art. 25/3. ; F. RAGAZZI *et al*., *op. cit*., p. 70.
[240] Loi du 5 août 1992 sur la fonction de police précitée, art. 44/1, §2, 1°.
[241] Loi du 5 août 1992 sur la fonction de police précitée, *ibidem.*
[242] M. KIMRI, P. LEGROS et C. LEQUESNE ROTH, *op. cit.*, p. 60.
[243] Loi du 5 août 1992 sur la fonction de police précitée, art. 44/2, §3, 1° et 2°, art. 44/11/3*sexies* à 44/11/3*decies*.

reste muette quant à la création d'une base de données pour les caméras intelligentes utilisant la reconnaissance faciale.

Par conséquent, la législation belge est sujette à interprétation : bien qu'elle autorise potentiellement l'utilisation de la technologie de reconnaissance faciale dans l'espace public, elle ne prévoit pas expressément la création d'une base de données spécifique à cette fin. Dans l'un de ses rapports, l'Organe de contrôle de l'information policière a fait le point sur la question et a affirmé que « le législateur a exclusivement voulu réglementer la création d'une banque de données technique pour les images ANPR »[244] et que dès lors, la loi actuelle n'a pas été élaborée en pensant à la reconnaissance faciale[245]. L'ancien premier ministre Koen Geens s'est également prononcé sur le sujet et a déclaré :

« Les données ANPR permettent de rechercher certains véhicules dans des zones bien précises et aussi, avec un peu de chance, les personnes qui s'y trouvent. La reconnaissance faciale permet, elle, de tracer simultanément des personnes – pour autant qu'elles se déplacent en public – à l'aide des dizaines de milliers de caméras. Il semble évident de renforcer davantage les régimes de contrôle sur ce type d'outils très performants. Selon les services de sécurité, cette technologie est encore loin d'être au point et ils ne pourront pas y avoir recours utilement avant un certain nombre d'années. »[246].

Par conséquent, il est nécessaire d'adapter le texte afin de permettre aux policiers d'utiliser les technologies de reconnaissance faciale comme moyen d'identification dans les espaces publics. Cette adaptation pourrait s'inspirer des règles applicables au recours de caméras intelligentes de reconnaissance automatique des plaques d'immatriculation, tout en prenant en compte les enjeux particuliers liés à l'utilisation de la reconnaissance faciale[247].

En adoptant une lecture a contrario de l'article 44/2, il est possible de conclure que celui-ci permet l'emploi d'un dispositif de reconnaissance faciale non relié à une base de données. En conséquence, l'utilisation de la reconnaissance faciale en tant que moyen d'authentification serait légalement envisageable pour les services de police, contrairement à son utilisation en

[244] Rapport intermédiaire avec mesure correctrice concernant la visite menée auprès de la police fédérale de l'aéroport de Zaventem par l'Organe de contrôle de l'information policière et portant sur l'utilisation de la reconnaissance faciale (DIO19004), disponible sur www.organedecontrole.be/publications/rapports, (ci-après abrégé « Rapport intermédiaire »), p. 4.
[245] F. RAGAZZI *et al*., *op. cit*., p. 71.
[246] Rapport intermédiaire, *op. cit.*, p. 4.
[247] M. KIMRI, P. LEGROS et C. LEQUESNE ROTH, *op. cit.*, p. 61.

tant que moyen d'identification, qui requiert nécessairement la création, même temporaire, d'une base de données liée au dispositif[248].

§3. L'utilisation des caméras de surveillances en dehors du contexte policier

La loi caméras règle quant à elle l'usage des technologies de reconnaissance faciale à des fins non policières. Elle prévoit précisément en son article 8.1 que « l'utilisation de caméras de surveillance intelligentes couplées à des registres ou à des fichiers de données à caractère personnel n'est autorisée qu'en vue de la reconnaissance automatique des plaques d'immatriculation ».

Ainsi, les autorités communales peuvent, par exemple, utiliser ces caméras de reconnaissance de plaques d'immatriculation pour prévenir et constater des incivilités en matière de stationnement ou autres infractions routières sanctionnées par des sanctions administratives communales, ainsi que pour contrôler le respect des règlements communaux concernant le stationnement payant[249]. Cependant, l'article est clair – l'utilisation de la reconnaissance faciale dans tous les autres cas est formellement interdite. Pour l'autoriser, il faudrait adopter une nouvelle loi ou modifier le texte.

Section 3. Position de l'Autorité de protection des données

En Belgique, l'autorité chargée de contrôler les traitements de données à caractère personnel, à l'exclusion des traitements effectués par les services de police et les services de sécurité, est l'Autorité de protection des données (ci-après « APD »). Cette dernière a été instituée par une loi du 3 décembre 2017[250] afin de remplacer la Commission de la protection de la vie privée[251], qui avait été mise en place en 1992. Très tôt la Commission avait commencé à s'intéresser aux traitements des données biométriques dans le cadre de l'authentification des individus. En effet, celle-ci avait rendu un avis en 2008[252] dans lequel elle soulignait la nécessité de réglementer rigoureusement le déploiement de la reconnaissance faciale en tant que méthode d'authentification, afin de respecter les principes de nécessité et de proportionnalité, tout en

---

[248] M. KIMRI, P. LEGROS et C. LEQUESNE ROTH, *ibidem.*, p. 61.
[249] Loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance précitée, art. 7.1. ; Police Locale Haute Senne, « Caméras de surveillance – Nouvelle règlementation ! », disponible sur www.police.be, 12 juillet 2018.
[250] Loi du 3 décembre 2017 portant création de l'Autorité de protection des données, *M.B.*, 10 janvier 2018.
[251] E. DEGRAVE, « Le R.G.P.D., les lois belges et le secteur public », *Le Règlement général sur la protection des données (R.G.P.D./G.D.P.R.) : premières applications et analyse sectorielle*, Liège, Anthemis, 2020, p. 308.
[252] Avis de la Commission de la vie privée relatif aux traitements de données biométriques dans le cadre de l'authentification des personnes (A/2008/017) du 9 avril 2008, disponible sur https://www.autoriteprotectiondonnees.be/publications/avis-n-17-2008.pdf.

garantissant sa légitimité. En l'absence d'une législation spécifique, cet avis rappelait les principes clés de protection des données personnelles qui devraient être pris en compte lors de la mise en place d'un tel dispositif[253].

En 2021, l'APD a publié une longue recommandation concernant, cette fois-ci, non seulement le traitement des données biométriques dans le cadre de l'authentification, mais également dans le cadre de l'identification. L'objectif principal de cette recommandation est d'aider les responsables du traitement et les sous-traitants à interpréter et appliquer correctement les règles du RGPD relatives au traitement de données biométriques[254]. De plus, la recommandation vise à encourager le législateur à établir une loi ou créer un article pour le traitement de données biométriques car actuellement, il existe une lacune dans la législation belge, de sorte que tout traitement de données biométriques sans le consentement explicite (à l'exception de celui réalisé dans le cadre de l'eID et du passeport) est effectué sans base légale. L'APD mentionne concrètement que le législateur belge devra spécifier dans la loi les conditions du traitement des données biométriques s'il souhaite autoriser leur utilisation dans des circonstances spécifiques[255].

Section 4. Perspectives législatives

Contrairement à la France qui prévoit d'adopter une loi visant à autoriser les systèmes de reconnaissance faciale à titre expérimental en amont des Jeux Olympiques de 2024[256], la Belgique n'a pas pris d'initiatives pour modifier son cadre juridique pour permettre l'utilisation de telles technologies. Toutefois, le 16 juin 2020, une proposition de résolution a été déposée en faveur 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[257]. La résolution appelle à un débat à la Chambre des représentants sur le sujet, afin d'établir un cadre approprié pour cette technologie avec des garanties strictes en matière de droits humains[258].

---

[253] M. KIMRI, P. LEGROS et C. LEQUESNE ROTH, *op. cit.*, p. 62 et 63.
[254] Autorité de protection des données, « Recommandation relative au traitement des données biométriques... », *op. cit.*, p. 3.
[255] Autorité de protection des données, *ibidem*, p. 4.
[256] Proposition de loi relative à la reconnaissance biométrique dans l'espace public, Rapport n°663, 2022-2023, déposé le 31 mai 2023, disponible sur https://www.senat.fr/rap/l22-663/l22-663_mono.html.
[257] Proposition de résolution 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.*, Ch., 2019-2020, n°1349/001.
[258] Développements précité, *Doc.*, Ch., 2019-2020, n°1349/001, p. 14.

Tant l'Organe de contrôle de l'information policière[259] que l'Autorité de protection des données[260] ont émis des avis concernant cette proposition. Dans un rapport plus approfondi que celui fourni par l'APD, le COC a exprimé ses arguments en faveur de la mise en place d'un moratoire. Il soulève notamment des inquiétudes quant à la légitimité de la police pour utiliser cette technologie[261], note le manque de soutien de la population envers son utilisation[262], met en évidence des problèmes persistants d'exactitude et de pertinence de la technologie[263], et souligne les risques pour les droits fondamentaux[264]. Ainsi, l'Organe de contrôle et l'Autorité de protection des données préconisent la suspension temporaire de cette pratique.

Ces différents points nous poussent à nous questionner quant à la pertinence de la Belgique d'envisager une législation future pour autoriser le traitement des données biométriques dans certains contextes. L'Organe de contrôle a considéré, à juste titre, qu'il « convient de se demander s'il est judicieux ou opportun de déjà légiférer au niveau national (belge) – du moins dans le but de parvenir à une législation définitive en matière d'intelligence artificielle ou de technologie de reconnaissance faciale – avant que le texte définitif du règlement européen sur l'intelligence artificielle n'ait été arrêté. En tout état de cause, une éventuelle législation nationale devra céder la place à la norme de droit internationale supérieure qu'est un règlement européen et en tenir compte. »[265]. L'autorité de protection des données semble partager cette opinion[266]. Il serait donc avisé que le législateur national opte pour une attitude d'attente, étant donné que légiférer sur des questions pouvant être modifiées en fonction des règles établies par l'AI Act pourrait se révéler peu judicieux.

[259] Avis de l'Organe de contrôle de l'information policière relatif à une proposition de résolution 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 1349/001) du 16 juin 2020, disponible sur https://www.organedecontrole.be/files/DA210029_Avis_F.pdf.
[260] Avis de l'Autorité de protection des données relatif à une proposition de résolution pour la mise en place d'un moratoire de trois ans sur l'utilisation de logiciels et d'algorithmes de reconnaissance faciale sur caméras de sécurité, fixes ou mobiles, dans les endroits publics et privés (n°248/2021) du 17 décembre 2021, disponible sur https://www.autoriteprotectiondonnees.be/publications/avis-n-248-2021.pdf.
[261] Avis de l'Organe de contrôle de l'information policière relatif à une proposition de résolution..., *op. cit*., p.16.
[262] Avis de l'Organe de contrôle de l'information policière relatif à une proposition de résolution..., *ibidem*, p.18.
[263] Avis de l'Organe de contrôle de l'information policière relatif à une proposition de résolution..., *ibidem,* p.19.
[264] Avis de l'Organe de contrôle de l'information policière relatif à une proposition de résolution..., *ibidem,* p.19.
[265] Avis de l'Organe de contrôle de l'information policière relatif à une proposition de résolution..., *ibidem*., p. 26.
[266] Avis de l'Autorité de protection des données relatif à une proposition de résolution..., *op. cit*., p. 3.

TITRE 3. ILLUSTRATION DES AFFAIRES RÉCENTES

La théorie ne correspond pas toujours à la réalité pratique. C'est précisément ce constat qui a suscité notre intérêt à examiner de manière approfondie quelques affaires significatives relatives à la sécurité publique qui ont surgi en Belgique durant ces dernières années. Ces affaires nous permettront d'analyser comment les acteurs impliqués ont interprété le cadre juridique existant et comment l'Organe de contrôle a traité ces situations délicates. Cette analyse nous donnera un aperçu concret des défis pratiques auxquels les acteurs de la reconnaissance faciale sont confrontés dans un contexte juridique parfois incertain, et mettra en lumière les éventuelles incohérences ou lacunes dans le cadre réglementaire actuel.

Nous procéderons ainsi à l'étude de deux affaires qui se sont déroulées à quelques mois d'intervalles – l'affaire Brussels Airport (chapitre 1) et l'affaire *Clearview AI* (chapitre 2).

CHAPITRE 1. L'AFFAIRE BRUSSELS AIRPORT

Au début de l'année 2017, Brussels Airport Company a acheté un logiciel de reconnaissance faciale pour la police fédérale de l'aéroport (ci-après « LPA ») afin de tester le système sur quatre caméras de surveillance. Les tests ont révélé une marge d'erreur importante avec des fausses correspondances, ce qui a entrainé l'arrêt du projet en mars 2017. En effet, des difficultés avaient été observées concernant la reconnaissance de la couleur de peau, des lunettes, ainsi que la détection de pilosité (moustache ou barbe)[267]. Malgré cela, le projet n'a pas été abandonné. Dans la première section de ce chapitre, nous examinerons en détail l'utilisation de la reconnaissance faciale par la LPA, cette fois-ci en 2019. La deuxième section se concentrera quant à elle, sur les éventuelles justifications légales de cette utilisation avec notamment l'examen du rapport de l'Organe de contrôle.

Section 1. Utilisation de la reconnaissance faciale par la LPA

Le 9 juillet 2019, le commissaire général Marc De Mesmaeker a annoncé dans une interview[268] que la police allait commencer à utiliser les caméras de reconnaissance faciale à l'aéroport de Zaventem. « Elles ont déjà aidé à résoudre rapidement des enquêtes, comme celle liée à la mort de Julie Van Espen. Les citoyens le comprennent et ont appris à vivre avec leur présence, mais le respect de la vie privée reste un droit. [...] Je reviens tout juste du Brésil et de

[267] Rapport intermédiaire, *op. cit.*, p. 3.
[268] J. LIPPENS et M. VANDERMISSEN, « Topman federale politie : 'We gaan camera's met gezichtsherkenning inzetten in Zaventem' », disponible sur www.knack.be, 9 juillet 2019.

Colombie. À l'aéroport de Sao Paolo, la douane effectue sa surveillance à l'aide de ces caméras. Les résultats sont impressionnants ! Le système repère les personnes qui ont un 'passif'. De la sorte, il n'est plus nécessaire d'avoir une centaine d'agents pour extraire aléatoirement des personnes des files. Nous allons introduire prochainement cette technologie à l'aéroport de Zaventem. Nous avons un accord avec l'exploitant et les syndicat. »[269], expliquait-il.

L'objectif était, selon le commissaire général, de renforcer la sécurité en utilisant un réseau de caméras connecté à un logiciel d'identification pour repérer les suspects en matière de terrorisme et de criminalité organisée, sans impliquer les passagers lambdas. En outre, la porte-parole de la police fédérale, Sarah Frederickx, a précisé dans la presse qu'il n'y aurait ni stockage, ni création de base de données. « De cette façon nous resterons dans le cadre juridique. Et c'est plus efficace de les traquer de cette manière. »[270].

L'Organe de contrôle, qui surveille l'usage policier des caméras, portait un autre regard sur l'initiative. « C'est effectivement possible si vous ne travaillez pas avec une base de données », confirmait Frank Schuermans, membre-conseiller de l'Organe de contrôle de l'information policière. « Mais cela reste une affaire délicate », expliquait-il[271].

Section 2. Bases légales et rapport de l'Organe de contrôle

Ce n'est qu'en visionnant l'interview sur l'hebdomadaire flamand *Knack* le 10 juillet 2019, que l'Organe de contrôle avait été mis au courant du déploiement de la reconnaissance faciale dans l'aéroport de Zaventem. Le commissaire général a été directement prié de transmettre tous les détails concernant le logiciel et son utilisation. Le 18 juillet 2019, le COC a reçu un résumé des principaux composants du système et a alors ensuite mené une visite le 9 août auprès de la police fédérale de l'aéroport de Zaventem[272].

Grâce au rapport publié par l'Organe suite à son enquête, nous avons connaissance de quelques détails techniques sur le système de reconnaissance faciale déployé à l'aéroport. Ce rapport explique que le système de reconnaissance faciale fonctionne en deux phases. Premièrement, lorsqu'il reçoit les flux vidéo des quatre caméras, le logiciel crée des

[269] X, « Des caméras avec reconnaissance faciale à Brussels Airport », disponible sur www.lalibre.be, 9 juillet 2019.
[270] T. BLANCMONT, « Aéroport de Bruxelles : reconnaissance faciale et Dashboard », disponible sur www.air-journal.fr, 11 juillet 2019.
[271] X, « La police lance une enquête sur le projet de caméras à reconnaissance faciale à Brussels Airport », disponible sur www.levif.be, 10 juillet 2019.
[272] Rapport intermédiaire, *op. cit.*, p. 3.

« *snapshots* »[273] en générant des enregistrements individuels avec les visages qui apparaissent dans le cadre. Deuxièmement, ces *snapshots* sont mis en correspondance avec des « listes noires » qui ont été préalablement créées par la police elle-même[274]. Comme nous l'avons mentionné précédemment, au début de l'année 2017, l'aéroport de Bruxelles a mis à disposition de la police fédérale de l'aéroport quatre caméras connectées à un logiciel de reconnaissance faciale. Cependant, le système n'a pas été à la hauteur de ses promesses. Il a produit un très grand nombre de faux positifs et a donc été débranché la même année. Toutefois, lors de la visite du COC en août 2019, il a été constaté que le système était toujours en partie actif, en ce sens qu'il collectait et stockait activement les données biométriques des visiteurs de l'aéroport de Bruxelles, mais sans les comparer cette fois-ci aux photos des listes noires[275].

Dans son courrier de réponse, le commissaire général de la police fédérale belge a fait valoir que, bien que le cadre juridique actuel ne permette pas la création d'une base de données technique, l'article 25/3 de la loi sur la fonction de police autorise l'utilisation de systèmes intelligents en temps réel. Pour rappel, cet article dispose que, dans l'exercice de leurs fonctions, les services de police peuvent recourir à des caméras fixes dans certains lieux publics, y compris les aéroports[276]. Le commissaire général insistait sur le fait que le texte précise expressément que ce genre de caméras peuvent être intelligentes[277].

Deux constats se dressent toutefois à cet égard. En premier lieu, le COC a fait valoir que pendant une période de test, il est loin d'être évident que la loi sur la fonction de police soit d'application, étant donné que le traitement de données à caractère personnel n'a pas pour objet la recherche ou la poursuite d'un délit[278]. En deuxième lieu, même si la loi sur la fonction de police était bel et bien applicable, cette dernière décrit ce qui doit être considéré comme une « caméra intelligente », mais elle ne précise pas les circonstances et les conditions d'utilisation de caméras permettant la reconnaissance faciale[279].

En outre, il est difficile d'imaginer comment un système de reconnaissance faciale en temps réel, tel que celui évoqué par le commissaire général, pourrait fonctionner, car il faudrait nécessairement maintenir une base de données pour stocker les images faciales, ce qui est illégal

[273] « (cliché) instantané », traduction sur www.larousse.fr.
[274] F. RAGAZZI *et al*., *op. cit*., p. 69. ; Rapport intermédiaire, *op. cit*., p. 3.
[275] Rapport intermédiaire, *ibidem*, p. 3.
[276] Loi du 5 août 1992 sur la fonction de police précitée, art. 25/3, 2°, b).
[277] Rapport intermédiaire, *op. cit.*, p. 4.
[278] Rapport intermédiaire, *ibidem,* p. 4.
[279] Rapport intermédiaire, *ibidem,* p. 4.

(à l'exception des banques de données ANPR)[280]. Il est également intéressant de constater que les *snapshots* générés n'ont été stockés que pendant une fraction de seconde, pourtant cela est tout de même considéré comme une base de données biométriques interdite en vertu de la loi[281].

Suite à ses observations, le COC a conclu que l'utilisation de caméras avec reconnaissance faciale à l'aéroport de Zaventem était illégale. En conséquence, une mesure correctrice a été ordonnée pour mettre fin à l'utilisation de ce type de système de traitement de données biométriques à partir de la date de la prise de connaissance de la décision[282].

CHAPITRE 2. L'AFFAIRE *CLEARVIEW AI*

En 2021, la police fédérale belge s'est retrouvée sous le feu des critiques suite à la divulgation de plusieurs documents compromettants révélant leur utilisation d'un logiciel de reconnaissance faciale particulièrement puissant – *Clearview AI*. Afin de mieux comprendre la controverse entourant cette application, nous nous pencherons dans un premier temps dans une brève présentation de ce logiciel (section 1). Nous continuerons ensuite par le cœur du sujet, à savoir l'utilisation de l'application par la police judiciaire fédérale (section 2). Enfin, nous examinerons le rapport exhaustif de l'Organe de contrôle de l'information policière (section 3).

Section 1. L'application controversée – *Clearview AI*

Clearview AI se définit comme « la plus grande base de données connue avec plus de 30 milliards d'images faciales provenant de sources exclusivement publiques sur le web, y compris les médias d'actualités, les sites web de photos d'identité judiciaire, les réseaux sociaux publics et de nombreuses autres sources ouvertes »[283]. La société collecte des images faciales et les stocke dans une énorme base de données qu'elle commercialise sous la forme d'un moteur de recherche. Ce dernier permet alors de rechercher n'importe quelle personne à partir d'une photo. La société propose ce service notamment aux services de police pour aider à identifier non seulement les responsables d'infraction, mais également les victimes[284].

---

[280] Loi du 5 août 1992 sur la fonction de police précitée, art. 44/2, §3 et 44/11/3*sexies* à 44/11/3*decies*. ; Rapport intermédiaire, *ibidem*, p. 4 et 5.
[281] F. RAGAZZI *et al.*, op. cit., p. 69.
[282] Rapport intermédiaire, *op. cit.*, p. 5.
[283] Traduction libre du site de Clearview AI, disponible sur https://www.clearview.ai/law-enforcement, consulté le 22 mars 2023.
[284] CNIL, « Reconnaissance faciale : sanction de 20 millions d'euros à l'encontre de Clearview AI », disponible sur www.cnil.fr, 20 octobre 2022.

Depuis sa création en 2019[285], la base de données de l'entreprise n'a cessé de s'agrandir de jour en jour. En effet, en quelques années seulement, *Clearview AI* est passé de 3 milliards d'images faciales à 30 milliards, comme en témoigne la dernière mise à jour du site. Hoan Ton-That, le créateur et le patron de *Clearview AI*, interrogé récemment sur les bienfaits de la technologie dans une interview[286], a expliqué comment l'application a été utilisée pour la première fois par un avocat qui cherchait à prouver l'innocence de son client. Ce dernier avait été condamné à tort à une peine de 15 ans de prison, en raison du manque de preuves et surtout en l'absence des coordonnées d'un témoin crucial. Même en fouillant partout, l'avocat ne parvenait pas à retrouver le témoin. Il a alors fait appel à *Clearview AI*, ce qui a permis de retrouver le témoin, rouvrir l'affaire et innocenter le client.

Face à cet exemple de résolution d'affaire criminelle, certains pourraient se demander pourquoi ce logiciel est sujet à de nombreux débats. *Clearview AI* est controversée car malgré le fait que les données utilisées soient accessibles publiquement, l'application soulève des préoccupations éthiques. En effet, les personnes dont les images et les données sont collectées ne sont probablement pas conscientes que leurs informations personnelles peuvent être si facilement extraites. La plupart des gens ne consentiraient pas à l'utilisation de leurs données à des fins de surveillance et d'identification. Toutefois, *Clearview AI* ne demande pas leur avis. Différents réseaux sociaux, dont Facebook et LinkedIn[287], ont d'ailleurs demandé à ce que *Clearview AI* mette un terme à la collecte de données sur leurs plateformes, considérant cela comme une violation de leurs politiques[288].

Section 2. L'utilisation de l'application par la police judiciaire fédérale

En octobre 2019, lors d'une réunion d'Europol à la Haye, deux enquêteurs de la police judiciaire fédérale ont été invités à tester le logiciel de *Clearview AI,* ce qu'ils ont accepté de faire sans anticiper les problèmes potentiels qui pourraient survenir[289]. Au début de l'année 2020, *Buzzfeed*, un site web américain, a pu accéder à une liste d'utilisateurs de la société

[285] H. TON-THAT, « The Modern Public Square: The Free Flow of Information in the Age of Artificial Intelligence », disponible sur www.clearview.ai,14 juin 2022.
[286] E. KIM SING, « An interview with CEO of Clearview AI, Hoan Ton-That », disponible sur www.identityweek.net, 14 décembre 2022.
[287] J. PORTER, « Facebook and LinkedIn are latest to demand Clearview stop scraping images for facial recognition tech », disponible sur www.theverge.com, 6 février 2020.
[288] M. CHARTIER, « La reconnaissance faciale : la technologie controversée de Clearview AI bientôt brevetée », disponible sur www.lesnumeriques.com, 6 décembre 2021.
[289] P. VAN LEEMPUTTEN, « Un audit sévère pour la police qui utilisa illégalement la reconnaissance faciale Clearview AI », disponible sur www.datanews.be, 10 mars 2022.

Clearview AI suite à une fuite de données. Cette liste indiquait notamment que la Belgique avait utilisé le logiciel. Toutefois, questionnées à l'époque, les autorités belges avaient rapidement nié cette information[290]. Plus d'un an après la fuite de données, *Buzzfeed* a ravivé le sujet en précisant que c'était la police judiciaire fédérale belge qui avait utilisé le logiciel de reconnaissance faciale « entre 101 et 500 fois » lors d'une réunion d'Europol[291]. *Data News* a alors contacté la police fédérale, mais cette dernière a de nouveau nié la connaissance d'une éventuelle utilisation de *Clearview AI* et a déclaré qu'elle n'avait même pas l'intention d'y recourir[292]. Suite à toutes ces informations, l'Organe de contrôle a réclamé à la police le lancement d'une enquête interne sur le sujet, et en cherchant mieux, la police a finalement admis avoir recouru au logiciel[293].

Suite à plusieurs questions parlementaires posées par différents partis tels que Vooruit, CD&V, PVDA-PTB, Ecolo, Groen, Vlaams Belang et PS, la ministre de l'Intérieur, Annelies Verlinden, avait également confirmé que le logiciel de reconnaissance faciale, qui demeure illégal, avait bel et bien été utilisé[294] : « En octobre 2019, dans le cadre d'une task force[295] d'Europol sur l'identification des victimes, deux enquêteurs ont eu accès à une licence d'essai valable pour une durée limitée »[296]. Selon Frank Schuermans, membre-conseiller du COC, ce type de recours à la technologie de reconnaissance faciale est très problématique. « Il n'y a pas de base légale juridique pour cela et il le savent. Même pour un test cela ne va pas. »[297], précisa-t-il.

Section 3. Analyse légale de l'affaire

§1. Absence de base légale au niveau national

Après des mois d'enquête concernant le recours à l'application de reconnaissance faciale par la police fédérale belge, le COC a rendu public son rapport de contrôle au mois de

[290] X, « La police belge réaffirme ne pas utiliser le logiciel Clearview AI », disponible sur www.lalibre.be, 28 août 2021.
[291] R. MAC et C. HASKINS, « Police In At Least 24 Countries Have Used Clearview AI. Find Out Which One Here », disponible sur www.buzzfeednews.com, 25 août 2021.
[292] P. VAN LEEMPUTTEN, « La Police Fédérale aurait utilisé le logiciel de reconnaissance faciale ClearView 'cent à cinq cents fois' (update) », disponible sur www.datanews.be, 27 août 2021.
[293] A. SENTE, « Reconnaissance faciale : la police belge admet avoir utilisé un logiciel controversé », disponible sur www.lesoir.be, 6 octobre 2021.
[294] P. VAN LEEMPUTTEN, « Verlinden : 'La police fédérale a quand même utilisé le logiciel de reconnaissance faciale Clearview AI' », disponible sur www.datanews.be, 8 octobre 2021.
[295] « La task force d'identification des victimes est une initiative d'Europol qui rassemble des spécialistes et des agences partenaires afin d'identifier les victimes et les délinquants représentés dans des documents sur les abus sexuels commis sur des enfants », disponible sur www.europol.europa.eu, 2022.
[296] A. SENTE, *op. cit*.
[297] A. SENTE, *ibidem*.

février 2022. Une analyse attentive de ce rapport révèle que la police judiciaire fédérale aurait effectué un total de 78 recherches avec le logiciel de *Clearview AI*, non seulement à La Haye, mais également dans leur bureau de la police fédérale[298], entre 2019 et la fin de la période d'essai du logiciel, le 10 février 2020[299].

Le commissaire général a été interrogé et a expliqué que les membres du personnel ont effectivement utilisé l'application *Clearview AI* mais sur des affaires non belges pendant leur participation à *la task force* d'Europol, ainsi que sur des dossiers du NCMEC[300] américain. Ils ont également effectué des tests avec leurs propres photos et celles de leurs collègues ou connaissances. Cependant, expliquait-il, ces tests n'ont jamais conduit à des résultats pertinents dans le cadre d'une enquête[301].

Dans ses conclusions d'enquête, le COC souligne que l'utilisation de la technologie *Clearview AI* sur des personnes qui n'ont pas la nationalité belge ne change rien au fait que l'absence d'une base légale suffisante dans la loi sur la fonction de police était problématique[302]. En effet, si le traitement effectué relève du champ d'application de l'Union européenne, la protection offerte par la directive en matière de protection des données dans le domaine répressif s'applique aux personnes physiques quelle que soit leur nationalité ou leur résidence[303].

L'Organe de contrôle poursuit en précisant que l'article 44/1 §2, 1° de la loi sur la fonction de police prévoit d'une manière générale le traitement de « données biométriques », mais ne fournit pas une « base légale suffisante » pour l'application de la reconnaissance faciale. Cela implique que l'utilisation de cette technologie présente un risque élevé pour la protection des droits et des libertés fondamentaux, conformément à la jurisprudence européenne qui exige une base légale spécifique et claire pour le traitement de données biométriques par des autorités répressives[304]. Par conséquent, en l'absence d'une telle base légale et de garanties adéquates en droit belge, le recours aux technologies de reconnaissance faciale est à l'heure actuelle interdit.

---

[298] J. NOULET et D. BRICHARD, « L'utilisation du logiciel de reconnaissance faciale « Clearview » par les policiers belges était illégale », disponible sur www.rtbf.be, 9 mars 2022.
[299] Rapport de contrôle de l'Organe de contrôle de l'information policière relatif à l'utilisation de l'application Clearview AI par la police intégrée (DIO21006), disponible sur www.organedecontrole.be/publications/rapports (ci-après abrégé « Rapport de contrôle »), p. 9.
[300] National Center for Missing and Exploited Children.
[301] Rapport de contrôle, *op. cit.*, p. 5.
[302] Rapport de contrôle, *ibidem*, p. 11.
[303] Considérant 2 de la directive (UE) 2016/680.
[304] Rapport de contrôle, *op. cit.*, p. 11.

§2. Clearview AI à la lumière du RGPD : portée et conformité de ses pratiques

A. Applicabilité du Règlement

Bien que plusieurs pays européens, dont la Belgique[305] et la France[306], aient mis en demeure ou aient infligé des amendes à *Clearview AI* en raison de plusieurs infractions au RGPD, l'entreprise ne semble pas vouloir se conformer à toutes ces injonctions européennes. L'entreprise justifie sa position en affirmant qu'elle n'est soumise qu'à la législation américaine et que les États-Unis ne l'ont jamais sanctionnée[307]. Par conséquent, il est légitime de se questionner sur la soumission des activités de *Clearview AI* aux règles du RGPD et sur la possibilité que l'entreprise puisse faire l'objet de sanctions.

La raison d'être de *Clearview AI* est la création et le développement d'une base de données à partir de photographies d'individus trouvées sur Internet. Conformément à l'article 4.1 du RGPD, « toute information se rapportant à une personne physique identifiée ou identifiable » constitue des données à caractère personnel. Comme nous l'avions observé antérieurement, les photographies traitées à des fins de reconnaissance faciale, deviennent des données biométriques, ce qui les classe parmi les données sensibles en raison de leur finalité de traitement[308]. Pourtant, est-ce que le RGPD trouve à s'appliquer à l'entreprise étant donné qu'elle n'est pas établie dans l'Union européenne ? En l'absence d'établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union[309], une entreprise étrangère peut tout de même être soumise au RGPD selon le critère dit de « ciblage »[310], lorsqu'elle cible des individus situés dans l'Union européenne soit pour offrir des biens et des services[311], soit pour surveiller leur comportement dans l'Union européenne[312]. Malgré le fait que *Clearview AI* ait principalement pour but d'identifier des individus, ses activités de traitement pourraient également englober la surveillance d'individus présents dans l'Union européenne. En effet, les images collectées par l'application sont généralement accompagnées de leurs sources, sous la forme de liens redirigeant vers les sites où les informations sont stockées. Cela permet également aux services de police, à un stade ultérieur, de surveiller les

[305] Rapport de contrôle, *ibidem,* p. 17.
[306] CNIL, « Reconnaissance faciale : sanction de 20 millions d'euros... », *op. cit*., 20 octobre 2022.
[307] X, « Reconnaissance faciale : le géant Clearview AI dans la tourmente », disponible sur www.lexpress.fr, 24 mai 2022.
[308] C. JASSERAND, « Clearview AI: illegally collecting and selling our faces in total impunity? (Part I) », disponible sur www.law.kuleuven.be, 28 avril 2022.
[309] Art. 3.1 du R.G.P.D.
[310] I. NERONI REZENDE, « Facial recognition in police hands: Assessing the 'Clearview Case' from a European perspective », *N.J.E.C.L*., Vol. 11, 2020, p. 379.
[311] Art. 3.2, a) du R.G.P.D.
[312] Art. 3.2, b) du R.G.P.D.

comportements en ligne des personnes sous surveillance, en dressant des profils dans le but de détecter leurs préférences et habitudes, ainsi que leurs lieux de résidence et leurs déplacements[313]. Par conséquent, nous pouvons supposer que *Clearview AI* pourrait potentiellement entreprendre des activités de traitement liées à la surveillance de personnes se trouvant dans un des États membres de l'UE au sens de l'article 3.2, b) du RGPD. Par ailleurs, il ne fait aucun doute que *Clearview AI* ait offert ses services à des clients dans l'UE, comme en témoigne le déploiement de son application par les autorités belges, cas que nous sommes en train d'analyser. Ces constats conduisent à la conclusion que les activités de *Clearview AI* sont bel et bien soumises au Règlement, et ce, même si elles ont lieu en dehors de l'Union européenne[314].

B. Licéité des pratiques

Compte tenu du fait que les activités de traitement se focalisent principalement sur une catégorie particulière de données personnelles, l'évaluation de la licéité des pratiques employées par *Clearview AI* se penchera sur les exigences énoncées à l'article 9 du RGPD. Sur son site Internet, l'entreprise déclare recueillir des images faciales exclusivement à partir du « web ouvert »[315], et elle précise ne pas effectuer de recherches ni être en mesure de récupérer des informations qui se veulent être confidentielles, telles que des photos se trouvant sur un compte Facebook ou Instagram restreint à des personnes spécifiques. De telles opérations peuvent sembler conformes à l'article 9 du RGPD, et plus particulièrement au deuxième paragraphe, lequel permet aux entreprises de traiter données qui ont été « manifestement rendues publiques par la personne concernée »[316]. C'est précisément en se basant sur cette justification que les deux policiers ont commencé à utiliser l'application. Ils ont supposé que les personnes qui publient du contenu accessible au public acceptent délibérément d'être contrôlées par la police, à l'instar des personnes qui visitent les lieux publics dans la réalité. Dans cette perspective, *Clearview AI* ne faisait que faciliter l'accès à des images qui sont déjà accessibles en ligne[317].

Toutefois, il est important de garder à l'esprit que le traitement doit être limité aux finalités pour lesquelles l'individu a volontairement partagé publiquement ses données personnelles[318]. Si ce principe n'est pas respecté, cela devient un détournement de finalité, étant donné que les

[313] I. NERONI REZENDE, *op. cit.*, p. 379.
[314] I. NERONI REZENDE, *ibidem*, p. 380.
[315] Voy. https://www.clearview.ai/legal.
[316] Art. 9.2, e) du R.G.P.D.
[317] Rapport de contrôle, *op. cit.*, p. 14.
[318] Art. 6 du R.G.P.D.

données sont alors traitées à des fins différentes de celles pour lesquelles elles ont été originellement recueillies. Lorsqu'une personne publie une photo sur un réseau social, il est peu concevable que son intention soit d'autoriser une société collaborant avec les services de police de collecter cette photo. Bien que la photo ait été intentionnellement rendue publique, la collecte de cette manière n'était pas du tout anticipée[319]. En tout état de cause, l'Organe de contrôle de l'information policière considère cette pratique comme contraire au cadre juridique actuel en matière de protection des données.

Section 4. Comparaison avec l'affaire Brussels Airport

Le rapport de contrôle du COC présente une comparaison entre les deux affaires impliquant l'utilisation de la technologie de reconnaissance faciale, l'une par la Direction générale de la police judiciaire (affaire *Clearview AI*) et l'autre par la Direction générale de la police administrative (affaire Brussels Airlines).

En premier lieu, l'Organe de contrôle constate que les deux affaires sont similaires car elles impliquent toutes les deux des traitements de données à caractère personnel effectués à des fins de test. Le COC continue en précisant que même pendant une phase de test ou un projet pilote, le traitement doit respecter la loi sur la protection des données ainsi que la loi sur la fonction de police. Il n'existe aucune dérogation possible au cadre légal[320]. Toutefois, dans l'avis concernant la proposition de résolution pour la mise en place d'un moratoire sur les technologies de reconnaissance faciale, le COC s'est montré favorable quant à la création d'un cadre législatif à l'égard des projets pilotes, et ce, sans attendre l'arrivée d'une éventuelle réglementation européenne sur le sujet. En effet, il considère qu'à l'heure actuelle, nous disposons que de très peu de moyens pour évaluer objectivement l'utilisation de telles technologies. C'est seulement après avoir mené un nombre suffisant d'essais, qu'il sera possible d'avoir une idée des pourcentages de faux positifs et de faux négatifs, des divers biais qui émergent, des limitations, etc[321]. Il est donc opportun, selon l'Organe, de permettre à la police fédérale judiciaire de tester la reconnaissance faciale, dans un cadre juridique bien établi, afin de comprendre le fonctionnement de cette technologie et d'en mesurer sa valeur ajoutée ainsi que sa performance dans notre société[322]. Le COC pourrait participer activement à ce cadre,

[319] C. JASSERAND, « Clearview AI: illegally collecting and selling our faces in total impunity? (Part II) », disponible sur www.law.kuleuven.be, 5 mai 2022.
[320] Rapport de contrôle, *op. cit.*, p. 13 et 14.
[321] Avis de l'Organe de contrôle de l'information policière relatif à une proposition de résolution..., *op. cit.,* p. 29
[322] Avis de l'Organe de contrôle de l'information policière relatif à une proposition de résolution..., *ibidem,* p. 28.

notamment à travers d'un mécanisme d'autorisation préalable. Cela impliquerait naturellement la réalisation d'une étude et d'un développement plus approfondi[323].

L'Organe de contrôle poursuit en donnant les différences principales entre les deux affaires. Tout d'abord, il constate que *Clearview AI* n'utilise pas la reconnaissance faciale sur des images provenant de caméras de surveillance installées dans des lieux publics, comme c'était le cas dans l'affaire de l'aéroport de Zaventem, mais elle se sert de photos ou d'images déjà en possession de la police dans le cadre de dossiers du NCMEC[324]. En outre, la police judiciaire fédérale a eu recours à une entreprise commerciale privée, *Clearview AI*, pour utiliser la technologie de reconnaissance faciale. Cela implique le transfert de données à caractère personnel policières à une tierce partie, sans qu'il ne soit prouvé que ce destinataire assure un niveau de protection suffisant ou qu'il offre les garanties nécessaires. Pourtant, d'après l'article 44/11/9 §1er de la LFP, seules des autorités publiques spécifiques sont autorisées à recevoir des données personnelles, excluant les entreprises commerciales privées[325]. Enfin, et cela va de pair avec le point précédent, le COC souligne que contrairement à l'utilisation de la reconnaissance faciale par la police fédérale dans l'affaire Brussels Airport, l'utilisateur de l'application *Clearview AI* n'a aucun contrôle sur le traitement des données biométriques. Les images faciales sont en effet chargées via une URL, ce qui signifie que la disponibilité des données est intégralement confiée à l'entreprise américaine. En conséquence, le service de police qui transmet les images, lui non plus n'a plus aucun contrôle sur le traitement des données personnelles. Il est donc fortement problématique que l'entité de police qui transmet les données à caractère personnel n'ait aucune influence sur le délai de conservation des photos, ni sur l'utilisation commerciale qui pourrait en être faite. En outre, il est pratiquement impossible pour les personnes concernées de savoir que leur photo a été utilisée par *Clearview AI.* Il est d'autant plus difficile pour elles d'exercer leurs droit à l'égard de cette application[326].

Section 5. Conclusion de l'affaire *Clearview AI*

Bien que *Clearview AI* ait sciemment contourné les réglementations en vigueur en Europe en autorisant les autorités belges à utiliser sa technologie de reconnaissance faciale au-delà des limites prévues, il semble qu'actuellement aucune sanction ne puisse être appliquée à l'entreprise. Malgré les poursuites judiciaires engagées et les décisions rendues par différentes

[323] Avis de l'Organe de contrôle de l'information policière relatif à une proposition de résolution..., *ibidem,* p. 29
[324] Rapport de contrôle, *op. cit*., p. 11.
[325] Rapport de contrôle, *ibidem*, p. 13.
[326] Rapport de contrôle, *ibidem*, p. 14.

autorités de protection des données, *Clearview AI* continue de mener ses activités sans préoccupations car elle n'a pas d'établissement physique sur le territoire de l'Union européenne. Il conviendra donc d'explorer d'autres alternatives pour mettre fin à ses opérations à l'avenir.

Jusqu'à présent, la seule mesure imposée par l'Organe de contrôle à la police fédérale belge est de « prendre les mesures et initiatives nécessaires au respect des obligations du responsable du traitement en cas d'atteinte à la sécurité de l'information »[327]. En outre, le COC met en garde la police fédérale contre toute éventuelle utilisation future de la technologie de reconnaissance faciale, soulignant que de telles actions seraient contraires à la loi[328].

Dans ce contexte, la question cruciale demeure de savoir comment les instances de régulation pourront efficacement contrôler les activités d'entreprises transnationales telles que *Clearview AI*, qui semblent échapper aux sanctions du fait de leur structure opérationnelle et légale complexe. Une coopération internationale plus étroite, ainsi que la mise en place de cadres juridiques plus solides pourraient s'avérer essentiels pour garantir la protection des droits individuels dans un environnement numérique en constante évolution.

[327] Rapport de contrôle, *ibidem,* p. 17.
[328] Rapport de contrôle, *ibidem*, p. 17.

CONCLUSION

Le présent mémoire posait la question de savoir si le cadre juridique actuel justifie la surveillance des individus au nom de la sécurité publique, dans le contexte de l'utilisation de la reconnaissance faciale dans les lieux publics.

Nous avons, dans une première partie, introduit les concepts fondamentaux associés à cette nouvelle technologie, en mettant en avant à la fois ses avantages et les préoccupations qu'elle suscite. Cela a permis de mieux appréhender les éléments clés tels que la biométrie, l'espace public et les différentes fonctions de la reconnaissance faciale. Au cours de cette analyse, il est apparu de manière évidente que la fonction d'identification des individus dans les espaces publics engendre un débat polarisé. D'un côté, ceux qui considèrent cette technologie comme une ressource inestimable dans la lutte contre la criminalité grâce à l'identification des individus et d'un autre, les défenseurs de la protection de la vie privée qui expriment des préoccupations légitimes quant aux possibles atteintes aux libertés individuelles. En effet, bien que la reconnaissance faciale offre des avantages indéniables, qu'il s'agisse de renforcer la sécurité lors d'un match de football au stade, de retrouver des meurtriers ou de s'assurer que mamie a correctement reçu sa dose de médicament, il est clair que la technologie demeure sujette à de nombreuses erreurs et biais, et de manière plus générale, soulève des inquiétudes quant à nos droits fondamentaux. Face à ces préoccupations, il est justifié de se demander si notre cadre réglementaire parvient efficacement à concilier l'équilibre délicat entre la sécurité potentielle apportée par l'utilisation des nouvelles technologies et le respect de la vie privée.

Ainsi, notre deuxième partie a examiné en détail le cadre juridique actuel des technologies de reconnaissance faciale. À l'échelle européenne, il n'existe actuellement pas de loi spécifique dédiée à ces technologies. Toutefois, étant donné que leur déploiement concerne des questions de vie privée et de protection des données personnelles, différentes normes contraignantes sont amenées à s'appliquer, dont le RGPD et la directive police-justice. Suite à une analyse minutieuse de ces dispositions, il ressort que malgré les principes fondamentaux qu'elles énoncent pour protéger nos images faciales, de nombreux problèmes et lacunes persistent. Cela est particulièrement évident en ce qui concerne la transparence : il existe peu d'informations sur le fonctionnement des systèmes biométriques, les fournisseurs d'applications ne sont soumis à aucune obligation, et il subsiste une incertitude quant aux institutions qui peuvent autoriser et contrôler les technologies de reconnaissance faciale. À cela

s'ajoute la disparité d'application du Règlement entre les États membres, ce qui ne contribue guère à renforcer la sécurité juridique dans ce domaine. Une avancée majeure a toutefois été réalisée, grâce à la proposition de législation européenne visant à mieux encadrer les nouvelles technologies émergentes sur le marché, et plus particulièrement, les technologies de reconnaissance faciale. Cependant, il est encore prématuré de dire quelle sera l'issue des négociations, étant donné que la Commission et le Conseil envisagent une interdiction de la reconnaissance faciale à distance et à temps réel dans les lieux publics, assortie à plusieurs exceptions liées à la sécurité publique, alors que le Parlement préconise une interdiction totale de cette pratique.

En ce qui concerne le droit belge, nous avons observé que l'utilisation de caméras intelligentes en dehors du contexte policier n'est autorisée qu'en vue de la reconnaissance automatique des plaques d'immatriculation. La question se complique d'avantage pour les services de police, qui se demandent s'ils peuvent ou non utiliser des caméras intelligentes. En vertu de la loi sur la fonction de police, leur utilisation est permise mais, pour la création d'une base de données seuls les systèmes de reconnaissance automatique des plaques d'immatriculation ont une base légale bien définie. Par conséquent, une zone de flou juridique persiste, comme cela avait été observé dans la troisième et dernière partie, lors de l'analyse des différentes affaires survenues en Belgique.

En effet, l'examen des test réalisés à l'aéroport de Zaventem, ainsi que ceux des essais effectués par la police fédérale avec le logiciel *Clearview AI*, ont confirmé l'existence de lacunes dans le cadre juridique actuel dans son application pratique. Ces failles soulèvent des problèmes significatifs car elles laissent place à des interprétations variées de la loi. Même le commissaire général de la police, qui joue un rôle central dans l'application de la loi, a tenté de « contourner » la législation en affirmant que celle-ci autorise explicitement l'usage de caméras intelligentes par les services de police. Heureusement l'intervention de l'Organe de contrôle a remis les pendules à l'heure en interdisant ces pratiques. Il est compréhensible que la police cherche à intégrer de nouvelles technologies pour faciliter l'exécution de ses missions. Toutefois, il est primordial d'adopter des lignes directrices précises avant d'entreprendre de telles initiatives, car l'utilisation de la reconnaissance faciale touche à des aspects sensibles et fondamentaux, notamment le droit à la vie privée.

Après avoir parcouru tous les éléments de ce raisonnement qui ont contribué à répondre à notre question de recherche, nous sommes en mesure de conclure que le cadre juridique, tel

qu'il est en vigueur aujourd'hui en Belgique, ne permet pas de justifier la surveillance des individus par le biais de la reconnaissance faciale car, actuellement, notre cadre juridique ne permet tout simplement pas l'utilisation de cette technologie. Toutefois, cette conclusion mérite d'être nuancée.

Premièrement, comme nous l'avons évoqué antérieurement, il n'est pas impossible qu'une législation autorisant des projets pilotes de reconnaissance faciale, à l'instar de celui de Zaventem, soit adoptée dans un futur proche. En effet, l'Organe de contrôle a souligné la pertinence d'établir un cadre juridique dédié à de tels essais, afin de permettre une meilleure compréhension du fonctionnement de cette technologie au sein des services de police. En lançant des projets pilotes bénéficiant d'une réglementation efficace, les autorités pourraient acquérir une expérience pratique ainsi que des informations quant à l'efficacité de la reconnaissance faciale dans la prévention et la résolution des infractions. Ces informations concrètes permettraient une évaluation objective de l'impact de cette technologie sur la sécurité publique. En outre, en ayant un cadre réglementaire strict en place, les données collectées pourraient ainsi être analysées de manière transparente, permettant donc une évaluation approfondie des enjeux potentiels et la prise de mesures correctives en temps voulu[329].

Deuxièmement, il reste envisageable que les négociations entre la Commission, le Conseil et le Parlement concernant l'*AI Act* débouchent sur une autorisation partielle de la reconnaissance faciale à des fins d'identification. Dans ce cas-là, si les autorités belges envisagent d'introduire des caméras intelligentes, la surveillance des individus serait permise mais sous des conditions bien précises, et ce, au nom de la sécurité publique. Selon notre point de vue, cette approche semble être la plus pragmatique. Une interdiction absolue des technologies de reconnaissance faciale ne semble plus réaliste à ce stade, étant donné que leur utilisation est déjà largement répandue à travers le monde, en Europe notamment, et plus particulièrement, au sein des services de police. De plus, bien que notre attention ait été principalement portée sur les aspects critiques de la reconnaissance faciale, il est indéniable que des résultats positifs pourraient émerger d'une utilisation éthique de cette technologie[330]. Ce qui se révèle nécessaire, c'est l'établissement de règles claires non seulement pour les fournisseurs, les vendeurs et les utilisateurs, mais aussi pour les citoyens qui occupent une position centrale dans cette dynamique. Il est essentiel d'informer au maximum tous ces

[329] Avis de l'Organe de contrôle de l'information policière relatif à une proposition de résolution..., *op. cit*., p. 28 et 29.
[330] J. SCIPIONE, « Has the horse bolted? Dealing with legal and practical challenges of facial recognition », *MediaLaws*, 2022, p. 3.

différents acteurs en élaborant un texte juridique transparent qui définit les différentes technologies envisagées, expose leur fonctionnement, identifie les potentiels risques qu'elles comportent, explicite les motifs précis de leur utilisation et détaille les mesures d'encadrement prévues. De plus, il est essentiel que la loi établisse des mécanismes de contrôles, et que la contre-vérification humaine en constitue une composante obligatoire et opérante. Il convient également de garder à l'esprit que le déploiement de la reconnaissance faciale demeure hautement intrusif et ne devrait pas être utilisé pour l'ensemble des délits – toutes les infractions ne justifient pas les risques inhérents. L'un des risques majeurs réside dans une utilisation quotidienne de la reconnaissance faciale, sans discernement, menant potentiellement à une surveillance de masse. Ainsi, il est impératif d'établir un seuil de gravité pour chaque infraction faisant l'objet d'une enquête, déterminant la pertinence de l'utilisation de la reconnaissance faciale, avec pour critère une peine légale minimale. La proposition de loi sur l'intelligence artificielle adopte déjà cette approche, néanmoins, la peine privative de liberté d'une durée maximale d'au moins trois ans semble modérée et permet d'inclure un large éventail d'infractions. Enfin, la personne faisant l'objet d'une enquête, de même que toutes les autres parties impliquées dans la procédure, doivent être informées de la participation d'une intelligence artificielle dans le processus d'identification, afin que chacun puisse adopter une stratégie de défense adéquate[331]. En mettant en place un tel cadre, la société dans son ensemble bénéficierait d'une meilleure compréhension, d'une protection accrue des droits individuels et favoriserait également une plus grande responsabilisation aussi bien des fournisseurs que des utilisateurs de ces technologies.

Pour finir, la question centrale entourant l'utilisation des technologies de reconnaissance faciale à des fins de sécurité publique souligne la nécessité d'une réflexion approfondie sur l'équilibre entre les avancées technologiques et les exigences éthiques. Alors que notre société évolue dans une ère de transformation numérique, l'établissement d'un cadre juridique rigoureux, la réflexion continue sur les normes éthiques et le maintien d'un dialogue entre les divers acteurs concernés se révèlent essentiels pour maintenir la démocratie et nos droits fondamentaux.

[331] J. SCIPIONE, *ibidem*, p. 3.

BIBLIOGRAPHIE

LÉGISLATION

Normes supranationales

- Charte des droits fondamentaux de l'Union européenne, signée à Nice le 7 décembre 2000.

- Règlement (CE) n° 2252/2004 du Conseil du 13 décembre 2004 établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres.

- Règlement (UE) 2016/679 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.

- Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, *J.O.U.E.*, L 119/89, 27 avril 2016.

- Proposition de règlement (UE) 2021/0106 du Parlement européen et du Conseil du 24 avril 2021 établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union.

- COM(2021) 205, Communication de la Commission au Parlement européen, au Conseil au Comité économique et social européen et au Comité des régions, « Favoriser une approche européenne en matière d'intelligence européenne », Bruxelles, 21 avril 2021.

Normes nationales

- Loi du 19 juillet 1991 relative aux registres de la population, aux cartes d'identité, aux cartes des étrangers et aux documents de séjour, *M.B.*, 3 septembre 1991.

- Loi du 5 août 1992 sur la fonction de police, *M.B.*, 22 décembre 1992.

- Loi du 8 décembre 1992 relative à la protection de la vie privée, *M.B.*, 18 mars 1993.

- Loi du 27 mars 2007 réglant l'installation et l'utilisation des caméras de surveillance, *M.B.*, 31 mai 2007.

- Loi du 3 décembre 2017 portant création de l'Autorité de protection des données, *M.B.*, 10 janvier 2018.

- Loi du 21 mars 2018 modifiant la loi sur la fonction de police, en vue de régler l'utilisation de caméras par les services de police, et modifiant la loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance, la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et la loi du 2 octobre 2017 réglementant la sécurité privée et particulière, *M.B.*, 16 avril 2018.

- Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements des données à caractère personnel, *M.B.*, 5 septembre 2018.

Documents parlementaires

- Projet de loi modifiant la loi sur la fonction de police, en vue de régler l'utilisation de caméras par les services de police, et modifiant la loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance, la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et la loi du 2 octobre 2017 réglementant la sécurité privée et particulière, *Doc.*, Ch., 2018, n°2855/001.

- Proposition de résolution 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.*, Ch., 2019-2020, n°1349/001.

Normes étrangères

- Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifié par l'Ordonnance n°2018-1125 du 12 décembre 2018, *J.O.*, 7 janvier 1978.

- Proposition de loi relative à la reconnaissance biométrique dans l'espace public, Rapport n°663, 2022-2023, déposé le 31 mai 2023, disponible sur https://www.senat.fr/rap/l22-663/l22-663_mono.html.

JURISPRUDENCE

- Cour eur. D.H. (gde ch.), arrêt *S. et Marper c. Royaume-Uni*, 4 décembre 2008, req. n° 30562/04 et 30566/04.

- C.J., arrêt *Productores de Música de España (Promusicae) c. Telefónica de España SAU*, 18 juillet 2007, C-275/06, EU:C:2008:54, Conclusions de l'avocat général Kokott, J., point 53.

- C.J. (gde ch.), arrêt *Volker und Markus Schecke et Eifert c. Land Hessen*, 9 novembre 2010, aff. jointes C-92/09 et C-93/09, EU:C:2010:662.

- Trib. administratif de Marseille, 27 février 2020, n°1901249, disponible sur www.doctrine.fr.

- Audiencia Provincial de Barcelona, Sección 9ª, Auto 72/2021 de 15 Feb. 2021, Rec. 840/2021, disponible sur https://diariolaley.laleynext.es/content/Documento.aspx?params=H4sIAAAAAAAEAMtMSbH1CjUwMDCzNDUwtzRVK0stKs7Mz7Mty0xPzStJBfEz0ypd8pNDKgtSbdMSc4pT1RKTivNzSktSQ4sybUOKSlMBe81L1EUAAAA=WKE.

DOCTRINE

- **ALMEIDA, D., SHMARKO K. et LOMAS, E.,** « The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU and UK regulatory frameworks », *AI and Ethics*, 2022, p. 377 à 387.

- **BERNARD, N. (dir.), BORN, R., DE JONGHE, D., DE TERWANGNE, C., MOREAU, P., SLINGENEYER, T., TRUFFIN, B., VAN MEERBEECK, J. et VANVREKOM, S.,** *Guide des citations, références et abréviations juridiques*, 6e éd., Bruxelles, Kluwer, 2017.

- **CASTELLUCCIA, C. et LE MÉTAYER, D.**, « Analyse des impacts de la reconnaissance faciale - Quelques éléments de méthode », *Inria*, 2019, p. 1 à 34.

- **CASTETS-RENARD, C.**, « Titre 2 - Réglementation des systèmes d'intelligence artificielle », *Droit du marché unique numérique et intelligence artificielle*, 1e édition, Bruxelles, Bruylant, 2020, p. 337 à 365.

- **CASTETS-RENARD, C. et BESSE, P.,** « Responsabilité *ex ante* de l'AI Act : entre certification et normalisation, à la recherche des droits fondamentaux au pays de la conformité », *Un droit de l'intelligence artificielle : entre règles sectorielles et régime général*, 1ère édition, Bruxelles, Bruylant, 2023, p. 597 à 628.

- **CHRÉTIEN, J., DROARD, E., FERNANDEZ, V., POUYAT, M.**, « Caméras "intelligentes" : N'ouvrons pas de nouvelles brèches dans notre Etat de droit », *Renaissance numérique*, 2022, p. 1 à 6.

- **CHRISTAKIS, T., BANNELIER, K., CASTELLUCCIA, C., LE MÉTAYER, D.**, « Mapping the Use of Facial Recognition in Public Spaces in Europe – Part 3: Facial Recognition for Authorisation Purposes », *Report of the AI- Regulation Chair - MIAI*, mai 2022, p. 1 à 54.

- **COWGILL, B. et DELL'ACQUA, F.**, « Biased programmers? Or biased data? A field experiment in operationalizing AI ethics », *Columbia Business School Research Paper Forthcoming*, 2020, p. 1 à 44.

- **DEGRAVE, E.,** « Le R.G.P.D., les lois belges et le secteur public », *Le Règlement général sur la protection des données (R.G.P.D./G.D.P.R.) : premières applications et analyse sectorielle*, Liège, Anthemis, 2020, p. 282 à 315.

- **DE HERT, P. et BOUCHAGIAR, G.,** « Visual and biometric surveillance in the EU. Saying 'no' to mass surveillance practice? », *Information Polity*, Vol. 27, 2022, p. 193 à 217.

- **DE TERWANGNE, C.,** « Présentation générale du R.G.P.D. et des lois belges relatives à la protection des données », *Le Règlement général sur la protection des données (R.G.P.D./G.D.P.R.) : premières applications et analyse sectorielle*, Liège, Anthemis, 2020, p. 7 à 58.

- **EYNARD, J.**, « Titre II - Le cadre juridique d'un schéma d'identification protecteur des droits et libertés », *L'identité numérique*, 1e édition, Bruxelles, Larcier, 2020, p. 159 à 206.

- **FONTES, C. et PERRONE, C.,** « Ethics of surveillance: harnessing the use of live facial recognition technologies in public spaces for law enforcement », *IEAI*, 2021, p. 1 à 11.

- **FUSSEY, P. et MURRAY, D.,** « Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology", *The Human Rights, Big Data and Technology Project*, 2019, p. 4 à 123.

- **GROTHER, P., NGAN, M. et HANAOKA, K.,** « Facial Recognition Vendor Test (FRVT). Part 3: Demographic Effects », *NLST*, 2019, p. 1 à 79.

- **HIROSE, M.,** « Privacy in Public Spaces: The Reasonable Expectation of Privacy Against the Dragnet Use of Facial Recognition Technology », *Connecticut Law Review*, Vol. 49, 2017, p. 1593 à 1620.

- **ISAAC, H. (dir.), VAZIAGA, C., CHRÉTIEN, J., FERNANDEZ, V., GALISSAIRE, J., LAUGIEZ, L., MORAT, G., POUYAT, M., RICHARD, A.,** « Reconnaissance faciale : porter les valeurs de l'Europe », *Renaissance numérique*, juin 2020, p. 5 à 98.

- **JACQUET, M. et GROSSRIEDER, L.**, « Enjeux et perspectives de la reconnaissance faciale en sciences criminelles », *Image et Justice*, Vol. 54, 2021, p. 136 à 170.

- **KIMRI, M., LEGROS, P. et LEQUESNE ROTH, C.**, « La Reconnaissance Faciale dans l'espace public – Une cartographie européenne », *Rapport de la Fablex DL4T*, avril 2020, p. 11 à 125.

- **KONSTANTINOS, K.,** « Facial recognition: A Challenge for Europe or a Threat to Human Rights? », *Eur. J. Privacy L. & Tech*., 2021, p. 142 à 156.

- **KRACHLER, A.,** « La proposition du règlement sur l'intelligence artificielle – Vers une intelligence artificielle maîtrisée par l'humain ? », *Rev. Aff. Eur*., 2022/3, p. 497 à 505.

- **MADIEGA, T. et MILDEBRATH, H.,** « Réglementation de la reconnaissance faciale au sein de l'Union européenne », *EPRS*, septembre 2021, p. 1 à 43.

- **MARTIN, A.,** « L'intelligence artificielle peut-elle être saisie par le droit de l'Union européenne ? », *Conférence Nationale en Intelligence Artificielle*, disponible sur http://hal.science, 2022, p. 1 à 11.

- **MENECEUR, Y.,** « Droits de l'Homme, numérique et intelligence artificielle – La perspective du Conseil de l'Europe », *Un droit de l'intelligence artificielle : entre règles sectorielles et régime général*, 1e édition, Bruxelles, Bruylant, 2023, p. 135 à 159.

- **MOBILIO, G.,** « Your face is not new to me – Regulating the surveillance power of facial recognition technologies », *Internet Policy Review*, 2023, p. 2 à 31.

- **MUCCHIELLI, L.,** « Note sur l'évaluation des nouvelles technologies de sécurité. Cas de la vidéosurveillance et de la reconnaissance faciale », *Laboratoire Méditerranéen de Sociologie*, 2019, p. 1 à 18.

- **NERONI REZENDE, I.,** « Facial recognition in police hands: Assessing the 'Clearview case' from a European perspective », *N.J.E.C.L.*, Vol. 11, 2020, p. 375 à 389.

- **NOROOZI, F. et TOYGAR, O.,** « Recognition of identical twins using fusion of various facial feature extractors », *EURASIP Journal on Image and Video Processing*, 2017, p. 1 à 14.

- **O'FLAHERTY, M**., « Facial recognition technology and fundamental rights », *EDPL*, 2020, p. 170 à 173.

- **POULLET, Y.,** *Le RGPD face aux défis de l'intelligence artificielle*, 1ère édition, Bruxelles, Larcier, 2020.

- **RAGAZZI, F. (dir), MENDOZ KUSKONMAZ, E., PLAJAS, I., VAN DE VEN, R. et WAGNER, B.,** « Biometric & Behavioural Mass Surveillance in EU Member States », disponible sur https://www.greens-efa.eu/biometricsurveillance/, 1 octobre 2021, p. 4 à 118.

- **RAPOSO, V.,** « The use of facial recognition technology by law enforcement in Europe: a non-Orwellian draft proposal », *European Journal on Criminal Policy and Research*, 2022, p. 1 à 19.

- **RAPOSO, V.**, « When facial recognition does not 'recognise': erroneous identifications and resulting liabilities », *AI & Society*, 2022, p. 1 à 13.

- **RAPOSO, V.,** « (Do not) remember my face: uses of facial recognition technology in light of the general data protection regulation », *Information & Communications Technology Law*, Vol. 23, 2023, p. 45 à 63.

- **SCHOENHER, D.**, « Reconnaissance faciale et contrôles préventifs sur la voie publique, l'enjeu de l'acceptabilité », *Les Notes du CREOGN,* 2019, N° 43, p. 1 à 4.

- **SCIPIONE, J.,** « Has the horse bolted? Dealing with legal and practical challenges of facial recognition », *MediaLaws*, 2022, p. 1 à 4.

- **SMITH, M. et MILLER, S.,** « The ethical application of biometrical recognition technology », *AI & Society,* Brighton*,* 2022, p. 167 à 175.

- **STROWEL, A.,** « L'intelligence artificielle : vers une régulation européenne par la gestion des risques », *Les pages : obligations, contrats et responsabilités*, Vol. 2021, no.99, p. 1.

- **WAELEN, R.,** « The struggle for recognition in the age of facial recognition technology », *AI and* Ethics, 2023, p. 215 à 222.

- **WONG, K. et DOBSON, A.,** « We're just data: Exploring China's social credit system in relation to digital platform ratings cultures in Westernized democracies », *Global Media and China Volume 4, Issue 2*, Sage Publications, 2019, p. 157 à 173.

AUTRE

Rapports et avis

- Rapport intermédiaire avec mesure correctrice concernant la visite menée auprès de la police fédérale de l'aéroport de Zaventem par l'Organe de contrôle de l'information policière et portant sur l'utilisation de la reconnaissance faciale (DIO19004), disponible sur www.organedecontrole.be/publications/rapports.

- Rapport de contrôle de l'Organe de contrôle de l'information policière relatif à l'utilisation de l'application Clearview AI par la police intégrée (DIO21006), disponible sur www.organedecontrole.be/publications/rapports.

- Avis de l'Organe de contrôle de l'information policière relatif à une proposition de résolution 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, disponible sur https://www.organedecontrole.be/files/DA210029_Avis_F.pdf.

- Avis de la Commission de la vie privée relatif aux traitements de données biométriques dans le cadre de l'authentification des personnes (A/2008/017) du 9 avril 2008, disponible sur https://www.autoriteprotectiondonnees.be/publications/avis-n-17-2008.pdf.

- Avis de l'Autorité de protection des données relatif à une proposition de résolution pour la mise en place d'un moratoire de trois ans sur l'utilisation de logiciels et d'algorithmes de reconnaissance faciale sur caméras de sécurité, fixes ou mobiles, dans les endroits publics et privés (n°248/2021) du 17 décembre 2021, disponible sur https://www.autoriteprotectiondonnees.be/publications/avis-n-248-2021.pdf.

Publications officielles européennes et nationales

- **AUTORITÉ DE PROTECTION DES DONNÉES**, « Recommandation relative au traitement de données biométriques », décembre 2021, disponible sur www.autoriteprotectiondonnees.be, p. 1 à 36.

- **AUTORITÉ DE PROTECTION DES DONNÉES**, « Reconnaissance faciale et droit à l'image », disponible sur www.autoritedeprotectiondesdonnees.be, s.*d.,* consulté le 2 mars 2023.

- **COMMISSION EUROPÉENNE,** « Study to Support an Impact Assessment of Regulatory Requirements for Artificial Intelligence in Europe. Final Report (D5) », disponible sur http://commission.europa.eu, avril 2021, p. 7 à 202.

- **COMMISSION EUROPÉENNE**, « Une Europe adaptée à l'ère du numérique : La Commission propose de nouvelles règles et actions en faveur de l'excellence et de la confiance dans l'intelligence artificielle », disponible sur https://ec.europa.eu, 21 avril 2021.

- **COMMISSION EUROPÉENNE**, « Peut-on traiter les données pour toutes les finalités ? », disponible sur https://commission.europa.eu/, *s.d.*, consulté le 20 mars 2023.

- **COMMISSION NATIONALE DE L'INFORMATION ET DES LIBERTÉS (CNIL)**, « Expérimentation de la reconnaissance faciale dans deux lycées : la CNIL précise sa position », disponible sur www.cnil.fr, 29 octobre 2019.

- **COMMISSION NATIONALE DE L'INFORMATION ET DES LIBERTÉS (CNIL)**, « Reconnaissance faciale – pour un débat à la hauteur des enjeux », disponible sur www.cnil.fr, 15 novembre 2019.

- **COMMISSION NATIONALE DE L'INFORMATION ET DES LIBERTÉS (CNIL)**, « Reconnaissance faciale : sanction de 20 millions d'euros à l'encontre de Clearview AI », disponible sur www.cnil.fr, 20 octobre 2022.

- **COMMISSION NATIONALE DE L'INFORMATION ET DES LIBERTÉS (CNIL)**, « Le cadre européen », disponible sur www.cnil.fr. *s.d.*, consulté le 12 juillet 2023.

- **COMMISSION NATIONALE DE L'INFORMATION ET DES LIBERTÉS (CNIL),** « Reconnaissance faciale », disponible sur www.cnil.fr, *s.d.*, consulté le 8 août 2023.

- **COUNCIL OF THE EUROPEAN UNION**, « Artificial Intelligence Act: Council calls for promoting safe AI that respects fundamental rights », disponible sur www.consilium.europa.eu, 6 décembre 2022.

- **EUROPEAN DIGITAL RIGHTS (EDRI),** « Ban Biometric Mass Surveillance. A set of fundamental rights demands for the European Commission and EU Member States », disponible sur https://edri.org, 13 mai 2020, p. 4 à 38.

- **FRA**, « Facial recognition technology: fundamental rights considerations in the context of law enforcement », *Publications Office of the European Union*, 2020, p. 1 à 36.

- **PARLEMENT EUROPÉEN**, « Loi sur l'IA de l'UE : première réglementation de l'intelligence artificielle », disponible sur www.europarl.europa.eu, 6 juin 2023.

Divers

- **ADA LOVELACE INSTITUTE,** « Beyond face value: public attitudes to facial recognition technology », disponible sur www.adalovelaceinstitute.org, septembre 2019.

- **ALLIX, G.,** « Comment des villes « hyper connectées » contrôlent l'espace public », *Le Monde*, 19 décembre 2018, disponible sur www.lemonde.fr, 19 décembre 2018.

- **BERTUZZI, L.,** « Le règlement de l'UE sur l'IA entre dans la phase finale du processus législatif », disponible sur www.euractiv.fr, 15 juin 2023.

- **BLANCMONT, T.**, « Aéroport de Bruxelles : reconnaissance faciale et Dashboard », disponible sur www.air-journal.fr, 11 juillet 2019.

- **CEST**, *Les enjeux éthiques soulevés par la reconnaissance faciale*, 8e commission jeunesse, disponible sur www.ethique.gouv.qc.ca, 2020.

- **CHARTIER, M.**, « La reconnaissance faciale : la technologie controversée de Clearview AI bientôt brevetée », disponible sur www.lesnumeriques.com, 6 décembre 2021.

- **CONLEY, J.,** « In 'Win for Fundamental Rights', EU Advances AI Rules Restricting Facial Recognition », disponible sur www.commondreams.org, 14 juin 2023.

- **DE RATH, R. et SADUTTO, M.**,« Vivons cachés : des logiciels de reconnaissance faciale utilisés par les polices européennes », disponible sur www.rtbf.be, 15 avril 2022.

- **GEORIS, V.,** « Le Parlement européen ne veut pas de la reconnaissance faciale par IA », disponible sur www.lecho.be, 14 juin 2023.

- **HARTZOG, W.,** « Facial recognition is the perfect tool for oppression », disponible sur http://cyberlaw.stanford.edu, 2 août 2018.

- **JASSERAND, C.,** « Clearview AI: illegally collecting and selling our faces in total impunity? (Part I) », disponible sur www.law.kuleuven.be, 28 avril 2022.

- **JASSERAND, C.,** « Clearview AI: illegally collecting and selling our faces in total impunity? (Part II) », disponible sur www.law.kuleuven.be, 5 mai 2022.

- **KIM SING, E.,** « An interview with CEO of Clearview AI, Hoan Ton-That », disponible sur www.identityweek.net, 14 décembre 2022.

- **LIPPENS, J. et VANDERMISSEN, M.,** « Topman federale politie: 'We gaan camera's met gezichtsherkenning inzetten in Zaventem' », disponible sur www.knack.be, 9 juillet 2019.

- **NOULET, J. et BRICHARD, D.,** « L'utilisation du logiciel de reconnaissance faciale « Clearview » par les policiers belges était illégale », disponible sur www.rtbf.be, 9 mars 2022.

- **MAC, R. et HASKINS, C.**, « Police In At Least 24 Countries Have Used Clearview AI. Find Out Which One Here », disponible sur www.buzzfeednews.com, 25 août 2021.

- **PIQUARD, A.,** « Intelligence artificielle : négociations tendues autour du projet de règlement européen AI Act », disponible sur www.lemonde.fr, 18 juillet 2023.

- **Police Locale Haute Senne**, « Caméras de surveillance – Nouvelle règlementation ! », disponible sur www.police.be, 12 juillet 2018.

- **PORTER, J.**, « Facebook and LinkedIn are latest to demand Clearview stop scraping images for facial recognition tech », disponible sur www.theverge.com, 6 février 2020.

- **SENTE, A.,** « Reconnaissance faciale : la police belge admet avoir utilisé un logiciel controversé », disponible sur www.lesoir.be, 6 octobre 2021.

- **SCHMITZ, B.,** « Le RWDM comme laboratoire pour une technologie de reconnaissance faciale », disponible sur www.rtbf.be, 5 septembre 2018.

- **STUBBE, P.**, « Het gebruik van facial recognition door de Belgische politiediensten », mémoire, Université de Gand, 2021-2022, p. 3 à 133.

- **TON-THAT, H.,** « The Modern Public Square: The Free Flow of Information in the Age of Artificial Intelligence », disponible sur www.clearview.ai,14 juin 2022.

- **VAN LEEMPUTTEN, P.**, « La Police Fédérale aurait utilisé le logiciel de reconnaissance faciale ClearView 'cent à cinq cents fois' (update) », disponible sur www.datanews.be, 27 août 2021.

- **VAN LEEMPUTTEN, P.,** « Verlinden : 'La police fédérale a quand même utilisé le logiciel de reconnaissance faciale Clearview AI' », disponible sur www.datanews.be, 8 octobre 2021.

- **VAN LEEMPUTTEN, P.**, « Un audit sévère pour la police qui utilisa illégalement la reconnaissance faciale Clearview AI », disponible sur www.datanews.be, 10 mars 2022.

- **WIEWIÓROWSKI, W.,** « Facial recognition: A solution in search of a problem? », disponible sur https://edps.europa.eu, 28 octobre 2019.

- **X**, « Des caméras avec reconnaissance faciale à Brussels Airport », disponible sur www.lalibre.be, 9 juillet 2019.

- **X**, « La police lance une enquête sur le projet de caméras à reconnaissance faciale à Brussels Airport », disponible sur www.levif.be, 10 juillet 2019.

- **X**, « La police fédérale doit mettre un terme à son projet de reconnaissance faciale à Zaventem », disponible sur www.lavenir.net, 20 septembre 2019.

- **X**, « La police belge réaffirme ne pas utiliser le logiciel Clearview AI », disponible sur www.lalibre.be, 28 août 2021.

- **X,** « Reconnaissance faciale : le géant Clearview AI dans la tourmente », disponible sur www.lexpress.fr, 24 mai 2022.

- **X,** « Guide to faster travel through the UK border », disponible sur www.gov.uk, 2 mai 2023.

LOUVAIN-LA-NEUVE | BRUXELLES | MONS | TOURNAI | CHARLEROI | NAMUR
Place Montesquieu, 2 bte L2.07.01, 1348 Louvain-la-Neuve, Belgique | **www.uclouvain.be/drt**