UCLouvain

Faculté de droit et de criminologie

La reconnaissance faciale à l'épreuve de l'AI Act : encadrement, dérives sécuritaires et protection des droits fondamentaux dans l'Union européenne

NOM et Prénom de l'étudiante : MATTHYS Lola
Promotrice : BEERNAERT Marie-Aude
Année académique 2024-2025
Master à finalité spécialisée en 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 107 à 114 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**.

Engagement d'intégrité – Travaux écrits et mémoires d'étudiant.e.s

Je reconnais avoir pris connaissance des règles d'or de l'honnêteté intellectuelle ainsi que des Lignes directrices sur l'usage responsable des outils d'intelligence artificielle de l'UCLouvain (disponibles sur le site www.uclouvain.be/drt - page "règlements") et je m'engage à respecter les valeurs d'intégrité et d'honnêteté qui fondent les règles et recommandations adoptées au sein de la communauté universitaire.

En particulier :

Engagement sur l'authenticité de mon mémoire/travail écrit

- Je déclare sur l'honneur que j'ai préparé et rédigé moi-même ce mémoire/travail écrit.

Reconnaissance du plagiat comme faute

- Je suis conscient·e que le plagiat consiste à réutiliser d'autres documents et sources, même partiellement, sans mentionner le nom de l'auteur ni/ou de la source. Reproduire littéralement des passages d'un autre document, éventuellement traduits, sans les placer entre guillemets, même si l'auteur et la source de cette œuvre sont mentionnés, constitue également un plagiat.
- Je reconnais que le plagiat constitue une faute grave qui entraîne l'application de la section 7 des articles 87 à 90 du Règlement général des études et des examens (RGEE).
- Je m'engage à ce que mon mémoire/travail ne constitue pas une reprise, même partielle, d'un autre document publié ou non, attribué à une personne ou anonyme.

Engagement à citer mes sources

- Je m'engage à attribuer à leur(s) auteur(s) toutes les idées, informations, données sur lesquelles je m'appuie. Je m'engage à référencer tous les emprunts intégrés au mémoire/travail (sous la forme de phrases, graphes, cartes, schémas, tableaux, etc.). Les références (par exemple, en note de bas de page) sont conformes aux exigences académiques et scientifiques (telles que présentées dans les cours de méthodologie, les séances de formation liées au Séminaire d'accompagnement des mémoires en Master et les guides de citation).

Engagement quant à l'usage d'outils d'intelligence artificielle (IA) générative

- Je m'engage à utiliser les outils d'IA générative, en particulier les générateurs de textes, de manière responsable, comme complément de mon apprentissage et sans chercher à contourner les exigences académiques.
- Je m'engage à respecter les Lignes directrices relatives à l'usage responsable de l'IA générative. Elles m'obligent notamment à référencer adéquatement les outils d'IA lorsque je reprends de manière littérale les contenus qu'ils ont générés. En revanche, certains usages de ces outils, par exemple comme assistant linguistique (pour corriger l'orthographe, la syntaxe ou le style), ne doivent pas être mentionnés.
- Je suis conscient·e que les contenus générés par ces outils d'IA ne reflètent pas nécessairement les faits/sources et je m'engage donc à toujours vérifier l'exactitude de ces contenus dans une démarche scientifique.
- Je m'engage à respecter toutes les consignes spécifiques pour le travail/mémoire, ainsi que les exigences de transparence et de documentation du processus ayant abouti au travail/mémoire, notamment en sauvegardant les conversations avec ces outils d'IA.
- Je m'engage à fournir, sur demande, des explications sur la manière dont j'ai utilisé ces outils.
- Je reconnais que le non-respect de ces exigences et de l'intégrité académique peut constituer un abus et être considéré comme une irrégularité au titre des articles 107 et suivants du RGEE et entraîner des sanctions telles que prévues aux articles 111 et suivants du RGEE.

Remerciements

Je souhaite avant tout remercier les personnes qui m'ont accompagnée tout au long de la rédaction de ce mémoire :

Ma promotrice, Madame Marie-Aude Beernaert, pour son suivi pédagogique, sa précieuse expertise et sa disponibilité,

Mes parents, à qui je dois tout, pour leur soutien sans faille sur absolument tous les plans, et pour avoir toujours cru en moi,

Chantal, ma taty, et Sophie, ma maman, pour le temps et le soin qu'elles ont consacrés à la relecture de tous mes travaux, et qui m'épaulent chaque jour,

Chloé, ma sœur, et Blaise, mon beau-frère et ami, pour leur écoute inconditionnelle et le réconfort qu'ils m'ont apporté.

Je n'oublie pas non plus mes amis, pour les mots d'encouragement et les moments de décompression partagés,

Particulièrement Valentine et Chloé, mes fidèles compagnes de blocus durant ces cinq années.

Table des matières

INTRODUCTION

Depuis sa création, l'intelligence artificielle connait un succès grandissant et occupe une place croissante dans nos sociétés. Celle-ci est perçue tantôt comme une formidable avancée technologique prometteuse, tantôt comme un dangereux outil qu'il faut restreindre et dont il faut se méfier. Nous la retrouvons dans de nombreux domaines : médical, scolaire, financier, pour n'en citer que quelques-uns, et finalement le domaine sécuritaire. Cette dernière application nous intéresse particulièrement dans l'écriture de cet ouvrage. Notre travail se concentre davantage sur son usage dans les lieux publics et à des fins répressives.

La reconnaissance faciale, technologie biométrique reposant sur l'intelligence artificielle, constitue un instrument incontournable dans cette quête de sécurité. En facilitant et en accélérant l'identification des individus au service de la surveillance de masse, elle accroît le contrôle des autorités et influence le comportement des citoyens, non sans conséquence sur leurs droits fondamentaux.

L'approche adoptée combine l'analyse doctrinale, l'étude de la jurisprudence ainsi que l'examen critique des textes législatifs belges et européens. Nous nous interrogeons principalement sur la conciliation entre d'une part, l'usage de la technologie de reconnaissance faciale, soutenue notamment par un besoin légitime de sécurité publique, et d'autre part, la préservation des libertés individuelles.

Ce mémoire se divise en trois parties. Premièrement, nous nous attelons à mettre la reconnaissance faciale en contexte. Pour ce faire, nous définissons certaines notions clés, exposons le fonctionnement de cette technologie, faisons état de son utilisation, en Belgique et ailleurs, et retraçons son historique.

La deuxième partie de ce travail se concentre sur l'encadrement législatif de la reconnaissance faciale par l'Union européenne. De nombreux états membres n'ont pas attendu que des normes soient adoptées et ont profité de ce vide juridique pour élaborer des projets pilotes et des expérimentations incluant la reconnaissance faciale. Dans un souci d'harmonisation et de sécurité juridique, l'Union européenne a récemment adopté un règlement régulant l'intelligence artificielle. Celle-ci a fait le choix d'une régulation basée sur le critère de risque. Nous analysons le cadre législatif, d'apparence restrictif, réservé à la reconnaissance faciale dans le domaine répressif.

Enfin, le dernier titre examine les conséquences de l'utilisation de la reconnaissance faciale sur les droits fondamentaux en mettant en lumière les risques de dérives et les discriminations potentielles. Nous présentons un aperçu des droits susceptibles d'être, ou déjà effectivement, compromis et nous interrogeons sur la légalité de ces atteintes.

Nous nous questionnons également sur l'efficacité réelle de ces technologies dans la réduction de la criminalité et de maintien de l'ordre public, ainsi que, plus largement, sur le concept de surveillance. Ces notions sont régulièrement avancées pour justifier le recours à la reconnaissance faciale. Finalement, nous explorons les stratégies de lutte adoptées par la société civile pour prévenir les abus d'un usage incontrôlé de ces technologies.

Ce travail juridique s'inscrit dans le projet de la Clinique Rosa Parks pour les droits humains. L'association « Ligue des droits humains » a exprimé des inquiétudes sur le sujet et entreprend diverses actions en ce sens. Par ce travail, nous entendons étayer et légitimer ces préoccupations tout en conservant une analyse critique et indépendante.

TITRE 1 : MISE EN CONTEXTE

Chapitre 1 : La reconnaissance faciale

Section 1 : Définitions

a) Vidéosurveillance

La première notion à définir est celle de « vidéosurveillance ». En effet, c'est par celle-ci que les technologies biométriques, notamment la reconnaissance faciale à des fins répressives, s'appliquent. La vidéosurveillance désigne « le système conçu pour surveiller à distance un espace déterminé à l'aide de caméras »[1]. On la définit également comme « un système de télévision dans lequel les signaux ne sont pas diffusés publiquement, mais sont traités principalement à des fins de surveillance et de sécurité »[2].

En vertu de la loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance, une caméra de surveillance est tout système d'observation fixe, fixe temporaire ou mobile, dont le but est la surveillance et le contrôle des lieux[3]. Ces caméras de surveillance traitent des images pour quatre finalités concrètes : « prévenir, constater ou déceler des infractions contre les personnes ou les biens », « prévenir, constater ou déceler des incivilités », « contrôler le respect des règlements communaux » ou « maintenir l'ordre public »[4].

b) Biométrie

La biométrie désigne l'ensemble des technologies informatiques utilisées pour identifier une personne en fonction de ses caractéristiques uniques et personnelles, notamment morphologiques, biologiques, physiologiques ou encore comportementales. Ces technologies se servent, par exemple, de la forme du visage ou de la main, du dessin de l'iris ou du doigt, des mouvements de l'écriture manuscrite ou encore de la signature vocale[5].

---

[1] E. HEILMANN, « La vidéosurveillance, un mirage technologique et politique », *in La frénésie sécuritaire : retour à l'ordre et nouveau contrôle social* (sous la dir. de L. MUCCHIELLI), Paris, La Découverte, 2008, p. 113.
[2] P. DE KEERSMAECKER et C. DEBAILLEUL, « The spatial distribution of open-street CCTV in the Brussels-Capital Region », *Brussels studies*, 2016, p. 1.
[3] Loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance, art. 2, 4°, *M.B.*, 31 mai 2007, p. 29529 ; J. TRULLEMANS, « Evaluation de la loi du 10 avril 1990 réglementant la sécurité privée et particulière : Compétences générales et situationnelles », *Postal Mémorialis*, 2023, p. 126.
[4] Loi du 21 mars 2007, précitée, art. 2, 4° ; J. TRULLEMANS, « Evaluation de la loi du 10 avril 1990 réglementant la sécurité privée et particulière : Compétences générales et situationnelles », *op. cit.*, p. 127.
[5] F. ROUSSET, « Biométrie et sécurité des installations sensibles », *Sécurité et stratégie*, 2018, p. 26.

La biométrie marque un tournant dans l'histoire de l'identité. Avec son avènement, nous retournons au corps et délaissons quelque peu les documents tels que la carte d'identité qui jusque-là constituait le principal moyen d'identification[6].

Cette innovation technologique nous permet l'accès à un nouvel outil, à une nouvelle approche du corps comme outil d'identification[7]. De nouveaux échantillons et fragments du corps permettent l'identification, nous entrons dans une métrique du corps[8].

c) Reconnaissance faciale

La reconnaissance faciale est une application particulière des technologies biométriques. Cette technologie a connu ses prémices dans les années 1970 mais s'est réellement développée dans les années 2010[9].

En France, la Commission nationale de l'informatique et des libertés (C.N.I.L.) la définit comme « une technique informatique et probabiliste qui permet de reconnaitre automatiquement une personne sur la base de son visage, pour l'authentifier ou l'identifier »[10]. La reconnaissance faciale est une technique parmi d'autres de traitement d'images vidéo. Alors que les simples caméras de vidéosurveillance se contentent de filmer les personnes et leur visage dans un espace déterminé, la reconnaissance faciale permet d'identifier automatiquement des individus[11].

Ce processus s'effectue en deux étapes. Premièrement, le visage est recueilli et traduit en un gabarit biométrique c'est-à-dire en un modèle informatique reflétant certaines caractéristiques du visage[12]. Ensuite, la reconnaissance peut s'effectuer en comparant le gabarit avec un ou plusieurs gabarits s'il s'agit d'une authentification ou d'une identification[13].

---

[6] B. FRAENKEL, « Un tournant biométrique ? » *in L'identification biométrique : champs, acteurs, enjeux et controverses* (sous la dir. de A. CEYAHN et P. PIAZZA), Paris, Editions de la maison des sciences de l'homme, 2011, p. 418.
[7] B. FRAENKEL, *op. cit*, p. 418.
[8] B. FRAENKEL, *op. cit.*, p. 419.
[9] R. CHATELLIER, « Des premières caméras à l'expérimentation des algorithmes : un panorama du développement territorial, technologique et de l'encadrement juridique de la vidéosurveillance », *Revue française d'administration publique*, 2024, p. 227.
[10] C.N.I.L., « Reconnaissance faciale : pour un débat à la hauteur des enjeux », 2019, p. 6, https://www.cnil.fr/fr/reconnaissance-faciale-pour-un-debat-la-hauteur-des-enjeux (date de dernière consultation : 1er avril 2025).
[11] C.N.I.L., « Reconnaissance faciale : pour un débat à la hauteur des enjeux », *op. cit.* p. 6.
[12] R. CHATELLIER, *op. cit.*, p. 227.
[13] R. CHATELLIER, *op. cit*, p. 227.

Cette technologie est fondée sur une estimation de comparaisons et de correspondances entre des modèles[14]. De cette opération, découle un degré de probabilité indiquant que la personne est celle dont l'identité est recherchée[15]. Lorsque ce degré dépasse un certain seuil, prédéfini par le système, celui-ci conclut à une correspondance[16].

d) Identification

La finalité primaire de cette technologie est l'identification des personnes. L'identification est une notion complexe et constitue un terme polysémique que nous pouvons retrouver notamment dans les domaines de la psychanalyse, de l'anthropologie, de la sociologie, de l'histoire[17]. Le droit n'est pas étranger à cette notion d'identification et est même amené à la réguler, à l'organiser. De plus, l'identité ne s'applique pas uniquement aux individus, mais peut également s'élargir aux groupes, aux territoires ainsi qu'aux institutions[18].

Du point de vue de l'historien, l'identification renvoie à l'acte de reconnaissance[19]. Nous parvenons à la reconnaissance en singularisant la personne c'est-à-dire en établissant ses caractères propres, et en la différenciant, autrement dit en la distinguant des autres individus[20]. L'identité ne peut être réduite à un état mais doit être perçue comme un processus s'appuyant sur la notion de « mêmeté » en interne et « d'altérité » par rapport à l'externe[21].

L'identification doit être distinguée de l'authentification. La première a pour but de joindre une identité à une personne, de définir qui elle est[22]. La seconde tend, quant à elle, à prouver que la personne est bien celle qu'elle prétend être[23]. Nous pourrions traduire l'identification comme étant un processus de repérage 1 parmi n, tandis que l'authentification est un processus d'appariement 1 avec 1[24].

---

[14] C.N.I.L., « Reconnaissance faciale : pour un débat à la hauteur des enjeux », *op. cit.* p. 6.
[15] C.N.I.L., « Reconnaissance faciale : pour un débat à la hauteur des enjeux », *op. cit.* p. 6.
[16] C.N.I.L., « Reconnaissance faciale : pour un débat à la hauteur des enjeux », *op. cit.* p. 6.
[17] I. ABOUT et V. DENIS, *Histoire de l'identification des personnes*, Paris, La Découverte, 2010, pp. 3-4.
[18] T. KERNALEGENN, « Identité », *in Dictionnaire encyclopédique de la décentralisation* (sous la dir. de N. KADA, R. PASQUIER, C. COURTECUISSE et V. AUBELLE), Boulogne-Billancourt, Berger-Levraut, 2017, p. 599.
[19] I. ABOUT et V. DENIS, *op. cit*, pp. 3-4.
[20] I. ABOUT et V. DENIS, *op. cit.*, pp. 3-4.
[21] T. KERNALEGENN, *op. cit.*, p. 599.
[22] F. ROUSSET, *op. cit.*, p. 27.
[23] F. ROUSSET, *op. cit.*, p. 27.
[24] R. CHATILA (e.a.), « Pourquoi la reconnaissance faciale, posturale et comportementale soulève-t-elle des questionnements éthiques » *in Pour une éthique du numérique* (sous la dir. de E. GERMAIN, C. KIRCHNER et C. TESSIER), Paris, Presses universitaires de France, 2022, pp. 211-212.

Section 2 : Processus

Nous allons tenter de nous familiariser avec le fonctionnement de la reconnaissance faciale. En comprenant le processus, nous pourrons mettre en lumière les enjeux que celle-ci fait naitre. Pour fonctionner, la reconnaissance faciale a besoin de trois éléments : un réseau de caméras de vidéosurveillance, un logiciel d'intelligence artificielle et une base de données biométriques[25].

a) Réseau de caméras de vidéosurveillance

Le premier élément indispensable à l'utilisation de la reconnaissance faciale est un support matériel. Indépendamment du cadre légal du recours à la reconnaissance faciale, une infrastructure matérielle adaptée, fonctionnelle et abondante est nécessaire[26]. En effet, c'est à partir des images recueillies que le processus d'identification pourra se mettre en marche.

Les caméras de vidéosurveillance constituent le dispositif de sécurité le plus répandu au sein de l'espace public[27]. Nous les rencontrons quotidiennement. Au début des années 1990, Bruxelles n'a pas fait exception aux autres villes européennes et les caméras de vidéosurveillance dans l'espace public ont fait leur apparition dans la capitale[28]. Depuis, ce réseau n'a cessé de se déployer par étapes successives, influencé par des enjeux de sécurité, de politique urbaine, d'économie et conforté par un cadre légal permissif[29].

Les caméras de vidéosurveillance sur la voie publique ne sont pas détenues uniquement par la police. D'autres institutions étatiques comme la STIB, la SNCB, Bruxelles Mobilité, le Port de Bruxelles, le SIAMU ainsi que De Lijn ou le TEC en disposent également[30]. En 2016, la Région Bruxelles-Capitale comptait déjà sur son territoire 8000 caméras et, pour ne citer que la STIB, celle-ci projetait d'atteindre les 15 000 dispositifs en 2025[31].

Il est également opportun de s'interroger sur la répartition géographique de ces caméras et d'analyser leur expansion sous une approche spatiale. A Bruxelles, une étude géographique a été réalisée. Celle-ci date de 2016 et depuis lors, aucune autre étude connue ou recensement

[25] Podcast « De quels droits on se chauffe. Fuyez, vous êtes identifié.es ! – épisode 1 » - Ligue des droits humains.
[26] Podcast « De quels droits on se chauffe. Fuyez, vous êtes identifié.es ! – épisode 1 » - Ligue des droits humains.
[27] R. CHATELLIER, *op. cit*, pp. 223-235.
[28] P. DE KEERSMAECKER et C. DEBAILLEUL, *op. cit.*, p. 1.
[29] P. DE KEERSMAECKER et C. DEBAILLEUL, *op. cit.*, p. 1.
[30] N. BOCQUET, « La Smart City à Bruxelles : quand 'intelligence' rime avec vidéosurveillance », *Brussels Studies*, 2021, p. 8.
[31] N. BOCQUET, *op. cit.*, p. 8.

précis du nombre de caméras, ainsi que leur répartition par zone de police, n'a été effectué mais nous pouvons tout de même en tirer des enseignements [32].

L'essentiel des dispositifs se situe dans le centre-ville de la capitale : au plus nous nous en éloignons au moins nous en retrouvons[33]. Cependant, la répartition n'est pas uniforme sur l'ensemble de la périphérie[34]. En effet, nous remarquons qu'une corrélation peut être établie entre les quartiers dits « populaires » dont le niveau de richesse est faible et une certaine concentration des caméras de vidéosurveillance[35]. De plus, ces quartiers sont généralement habités par une population immigrée[36].

En conclusion, les habitants d'une même ville ne sont pas soumis à la même surveillance. Nous approfondirons les conséquences d'une telle disparité dans l'installation de ces dispositifs dans la suite de ce travail.

b) Logiciel

La vidéosurveillance est exponentiellement utilisée et mise en place à des fins sécuritaires[37]. Il en découle que de plus en plus d'images vidéos sont produites et que le volume des données augmente continuellement[38]. Il y a 10 ans, nous comptions 245 millions de caméras de surveillance sur le globe[39]. En l'espace de 4 ans, le volume d'information a doublé, passant de 860 pétaoctets en 2017 alors qu'il s'élevait à 413 pétaoctets en 2013[40].

Afin d'analyser l'ensemble de ces images qui ne cessera de s'accroître, un nombre conséquent de personnes devra être embauché[41]. De plus, la concentration et l'attention des opérateurs chargés de visionner durant de longues heures diminuent rapidement au fil du temps[42]. En effet, après seulement 12 minutes de visionnage d'images de vidéosurveillance, l'opérateur manquera jusqu'à 45% de l'activité de l'écran[43]. Au-delà des 22 minutes de

[32] N. BOCQUET, *op. cit.*, p. 9.
[33] Podcast « De quels droits on se chauffe. Fuyez, vous êtes identifié.es ! – épisode 1 » - Ligue des droits humains ; P. DE KEERSMAECKER et C. DEBAILLEUL, *op. cit.*, p. 5.
[34] Podcast « De quels droits on se chauffe. Fuyez, vous êtes identifié.es ! – épisode 1 » - Ligue des droits humains ; P. DE KEERSMAECKER et C. DEBAILLEUL, *op. cit.*, p. 5.
[35] P. DE KEERSMAECKER et C. DEBAILLEUL, *op. cit.*, p. 4.
[36] P. DE KEERSMAECKER et C. DEBAILLEUL, *op. cit.*, p. 4.
[37] Organisation de coopération et de développement économique, *L'intelligence artificielle dans la société*, Paris, Editions de l'OCDE, 2019, p. 78.
[38] Organisation de cooperation et de développement économique, *op. cit.*, p. 78.
[39] Organisation de cooperation et de développement économique, *op. cit.*., p. 78.
[40] Organisation de cooperation et de développement économique, *op. cit.*., p. 78.
[41] Podcast « De quels droits on se chauffe. Fuyez, vous êtes identifié.es ! – épisode 1 » - Ligue des droits humains.
[42] P. LÉGLISE, « Le défi de l'encadrement juridique de l'IA : l'exemple de l'expérimentation de la vidéoprotection intelligente », *Servir*, 2024, p. 27.
[43] P. LÉGLISE, *op. cit.*., p. 27.

visionnage, ce pourcentage peut s'élever jusqu'à 95%[44]. Nous en sommes réduits au constat, qu'humainement, il n'est pas possible de traiter des quantités d'informations aussi importantes et d'effectuer une identification par reconnaissance faciale[45].

Pour pallier cela, des entreprises ont créé des logiciels d'analyse d'images à détection automatique[46]. Ces logiciels ne se limitent pas à effectuer une reconnaissance faciale ; certains sont capables de reconnaitre des émotions et des comportements. En France, l'entreprise Thalès développe un projet nommé « Safecity ». Pour ce faire, elle a mis sur pieds des caméras prédictives, détectrices de coup de feu et de présence[47]. La start-up, également française, « Two-i » a mis au point un logiciel capable d'analyser les émotions en temps réel des usagers des transports en commun et ainsi repérer les expressions faciales inquiètes[48].

En réalité, nous pouvons distinguer les caméras dites « augmentées », des caméras biométriques[49]. Les caméras augmentées catégorisent et analysent par l'intermédiaire de l'intelligence artificielle mais, à l'inverse des caméras biométriques, elles n'identifient pas une personne de manière unique[50]. Ces dernières traitent des données sensibles et sont donc plus fortement réglementées[51].

c) Banque de données biométriques

Le dernier élément nécessaire à l'utilisation de la reconnaissance faciale est une base de données policières afin de réaliser une comparaison et de potentiellement conclure à une concordance[52]. Plusieurs bases de données ont été créées par les autorités fédérales et rassemblent des données à caractère personnel des citoyens[53]. Aujourd'hui, nous comptons cinq types de banques de données policières en Belgique : la banque nationale générale, les banques de données de base, les banques de données particulières, les banques de données communes et finalement les banques de données techniques[54].

---

[44] P. LÉGLISE, *op. cit.*, p. 27.
[45] Organisation de cooperation et de développement économique, *op. cit.*, p. 78.
[46] Podcast « De quels droits on se chauffe. Fuyez, vous êtes identifié.es ! – épisode 1 » - Ligue des droits humains.
[47] M. DENIAU, « Entretien avec Drago : Les villes connectées fliquent l'espace public », *Silences*, 2020, pp. 46-48.
[48] M. DENIAU, *op. cit.*, pp. 46-48.
[49] C.N.I.L., « Les caméras 'augmentées' ou algorithmiques dans l'espace public », 2024, https://www.cnil.fr/fr/cameras-augmentees-espaces-publics (date de dernière consultation : 25 février 2025).
[50] C.N.I.L., « Les caméras 'augmentées' ou algorithmiques dans l'espace public », *op. cit.*
[51] C.N.I.L., « Les caméras 'augmentées' ou algorithmiques dans l'espace public », *op. cit.*
[52] Podcast « De quels droits on se chauffe. Fuyez, vous êtes identifié.es ! – épisode 1 » - Ligue des droits humains.
[53] MyData, « Votre plateforme sur la transparence des données fédérales », https://mydata.belgium.be/fr/ (date dernière consultation : 25 février 2025).
[54] F. DUMORTIER, « L'accès aux données policières : un droit (in)direct susceptible de recours effectif », *DPO news*, 2023, p. 15.

Le règlement général sur la protection des données[55], la loi sur la fonction de police[56] ainsi que la loi du 30 juillet 2018 sur la protection des données[57], transposant la directive 2016/680 appelée directive « police-justice »[58], organisent et réglementent le traitement des données[59]. L'Organe de contrôle de l'information policière est une autorité indépendante qui se charge de contrôler le respect de ces normes[60].

Toutes ces bases de données sont administrées par un responsable de traitement distinct[61]. Il est toutefois complexe pour la personne faisant l'objet d'un traitement de ses données, susceptible de l'affecter, d'identifier le responsable de traitement et en conséquence, le pouvoir d'information du sujet est mis à mal[62].

Chapitre 2 : Utilisation de ces technologies avant l'AI Act

Section 1 : En Belgique

a) Vidéosurveillance « classique »

Comme exposé dans le chapitre précédent, nous retrouvons en Belgique de nombreuses caméras de vidéosurveillance. L'installation et l'utilisation des caméras de surveillance ont été réglées par la loi du 21 mars 2007, appelée la « loi caméras »[63]. L'article 2 de cette loi délimite le champ d'application. Il dispose que sont sujettes les caméras ayant pour finalité de : « 1° prévenir, constater ou déceler des infractions contre les personnes ou les biens ; 2° prévenir, constater, ou déceler des incivilités au sens de l'article 135 de la nouvelle loi communale, contrôler le respect des règlements communaux ou maintenir l'ordre public »[64].

---

[55] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, *J.O.U.E.*, 4 mai 2016, L 119, pp. 1-88.
[56] Loi du 5 août 1992 sur la fonction de police, *M.B.*, 22 décembre 1992, p. 27124.
[57] 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, p. 68616.
[58] Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection 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.*, 4 mai 2016, L 119, pp. 89-131.
[59] C. FORGET, « L'effacement des données policières et judiciaires : un parcours du combattant ? », *e-legal Revue de droit et de criminologie de l'ULB*, 2022, p. 3.
[60] C. FORGET, *op. cit.*., p. 3.
[61] F. DUMORTIER, *op. cit.*., p. 15.
[62] F. DUMORTIER, *op. cit.*., p. 15.
[63] Loi du 21 mars 2007, précitée.
[64] Loi du 21 mars 2007, précitée, art. 2, 4°.

Cependant, certaines caméras de surveillance ne tombent pas sous ce champ d'application et doivent suivre les prescrits d'autres législations[65]. En effet, en vertu de l'article 3, cette loi n'est pas applicable aux caméras de surveillance dont les modalités d'installation et d'utilisation sont réglées par une législation particulière, aux caméras de surveillance sur le lieu de travail, ainsi qu'aux caméras de surveillance installées et utilisées par les services publics d'inspection et de contrôle[66].

Lorsque les caméras sont utilisées par les services de police, en raison de leurs missions spécifiques, il ne faut pas avoir égard à la loi caméras du 21 mars 2007[67]. Le législateur a considéré que cette dernière était trop restrictive et a alors ajouté un régime particulier pour l'utilisation par les services de police de caméras fixes et mobiles[68]. Ces dispositions particulières ont été insérées dans la loi sur la fonction de police du 5 août 1992[69]. De plus, cette législation précise que l'utilisation des caméras par la police ne relève pas de la compétence de l'Autorité de protection des données, mais d'une autorité publique spécifique : l'Organe de contrôle de l'information policière[70].

Les utilisateurs et installateurs de caméras de surveillance sont soumis à certaines obligations légales. Il est notamment interdit d'utiliser une caméra de surveillance cachée. On considère comme cachée « toute utilisation de caméras de surveillance qui n'a pas été autorisée au préalable par la personne filmée ou, (…) qui ne respecte pas les modalités de signalisation (…) »[71]. L'article 8 de la loi caméras précise qu'il y a une présomption d'autorisation lorsqu'un individu pénètre dans un lieu où un pictogramme signale l'existence d'une surveillance par caméra[72]. Il existe cependant des exceptions lorsque ces caméras font l'objet d'une utilisation policière. La loi sur la fonction de police dispose que, moyennant une autorisation préalable, des caméras peuvent être utilisées de manière non visible « lorsque les circonstances ne permettent pas aux fonctionnaires de police d'être identifiables ou sont de nature à rendre inopérante l'utilisation de caméras de surveillance de manière visible »[73]. La police peut

[65] J. TRULLEMANS, « Evaluation de la loi du 10 avril 1990 réglementant la sécurité privée et particulière : Compétences générales et situationnelles », *op. cit.*, p. 127.
[66] Loi du 21 mars 2007, précitée, art. 3, al. 2.
[67] J. TRULLEMANS, « Evaluation de la loi du 10 avril 1990 réglementant la sécurité privée et particulière : Compétences générales et situationnelles », *op. cit.*., p. 128.
[68] P. LAMBERT, « L'utilisation de caméras par les services de police, dans le cadre de la loi sur la fonction de police du 5 août 1992 », *Postal Mémorialis*, 2020, p. 62.
[69] Loi du 5 août 1992, précitée.
[70] Loi du 5 août 1992, précitée, art. 46/1. J. TRULLEMANS, « Evaluation de la loi du 10 avril 1990 réglementant la sécurité privée et particulière : Compétences générales et situationnelles », *op. cit.*., p. 128.
[71] Loi du 21 mars 2007, précitée, art. 8, al. 1er et 2.
[72] Loi du 21 mars 2007, précitée, art. 8, al. 3.
[73] Loi du 5 août 1992, précitée, art. 46/4.

également avoir recours aux caméras non visibles lors de la préparation d'actions de police judiciaire ou du maintien de l'ordre public lors de celles-ci[74], dans le cadre de l'exécution de missions spécialisées de protection de personnes[75] ou encore dans le cadre du transfert de personnes arrêtées ou détenues[76]. L'Organe de contrôle de l'information policière doit être notifié de l'utilisation de caméras non visibles, celui-ci est doté d'un pouvoir spécial quant à leur utilisation[77]. Cette obligation de notification ne s'applique cependant qu'à la police administrative et non à la police judiciaire ; cette dernière étant déjà chapeautée par un magistrat[78]. L'Organe de contrôle évalue la légitimité de l'utilisation, la prolongation, de la caméra non visible, le respect des conditions légales et le cas échéant y met un terme ou la suspend[79].

b) Caméras intelligentes

La loi caméras et la loi sur la fonction de police définissent la caméra intelligente comme étant « la caméra qui comprend également des composantes ainsi que des logiciels qui, couplés ou non à des registres ou à des fichiers, peuvent traiter de manière autonome ou non les images recueillies »[80]. Cette définition concerne donc autant des caméras qui ne sont capables que de détecter des bruits ou mouvements, et qui ont donc un impact limité et mesuré sur la vie privée des individus, que des caméras qui, via un accès à une base de données à caractère personnel, effectuent une reconnaissance faciale ou de plaques minéralogiques, constituant une atteinte et une menace plus importante sur les droits fondamentaux des citoyens[81].

La loi caméras dispose 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, à condition que le responsable du traitement traite ces registres ou ces fichiers dans le respect de la réglementation relative à la protection de la vie privée »[82]. Cet article fait suite à la révision

[74] Loi du 5 août 1992, précitée, art. 46/7.
[75] Loi du 5 août 1992, précitée, art. 46/9.
[76] Loi du 5 août 1992, précitée, art. 46/11.
[77] Organe de contrôle de l'information judiciaire, « Législation relative à l'usage de caméras », https://www.organedecontrole.be/services-de-police/l%C3%A9gislation-relative-%C3%A0-lusage-de-cam%C3%A9ras (date de dernière consultation : 2 mars 2025).
[78] Organe de contrôle de l'information judiciaire, « Législation relative à l'usage de caméras », *op. cit.*
[79] Organe de contrôle de l'information judiciaire, « Législation relative à l'usage de caméras », *op. cit.*
[80] Loi du 5 août 1992, précitée, art. 25/2, §1er, 3° ; Loi du 21 mars 2007, précitée, art. 2, 4°/3.
[81] A. MICHEL, « Révision de la loi caméras : précisions ou ambiguïtés pour l'installation et l'utilisation de caméras de surveillance ? », *J.T.*, 2019, pp. 149-160.
[82] Loi du 21 mars 2007, précitée, art. 8/1.

de la loi caméras[83] dont l'un des objectifs principaux était de s'adapter au développement de la technologie et d'offrir alors un cadre légal aux caméras intelligentes[84]. Un timide encadrement légal a alors vu le jour. Un seul cas de figure d'utilisation de caméras intelligentes a été autorisé : celles permettant la reconnaissance automatique des plaques d'immatriculation[85]. Ces caméras sont dotées de la technologie ANPR, qui est l'acronyme d'Automatic Number Plate Recognition.

En 2018, la police intégrée exprimait le souhait de renforcer la sécurité routière afin de limiter le nombre de décès sur les routes[86]. Pour ce faire, elle comptait développer l'automatisation des contrôles routiers, des constatations et du traitement grâce aux nouvelles technologies[87]. Parmi ces nouvelles technologies, nous retrouvons les caméras ANPR « permettant à la police de rechercher des véhicules non immatriculés, non assurés ou sans certificat valable, et d'intercepter les personnes qui ne respectent pas leur déchéance du droit de conduire »[88]. Ces caméras ont également d'autres utilisations : elles peuvent permettre aux communes de restreindre certaines zones dans lesquelles les automobilistes peuvent ou non accéder. Le respect des panneaux routiers indiquant un accès interdit ou le commencement d'une zone piétonne est contrôlé par des caméras à reconnaissance de plaque minéralogique[89]. Les communes peuvent également y avoir recours afin de prévenir, constater ou déceler des incivilités et pour contrôler le respect des règlements communaux en matière de stationnement payant[90].

Récemment, il a été question de mettre à contribution ces caméras afin de sanctionner les personnes utilisant leur téléphone au volant[91]. En 2021, une proposition de loi a été déposée afin d'établir un cadre juridique permettant à l'intelligence artificielle de repérer

---

[83] 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, p. 33691.
[84] A. MICHEL, *op. cit.*, pp. 149-160.
[85] A. MICHEL, *op. cit.*., pp. 149-160.
[86] J. TRULLEMANS, « Plan national de sécurité : Groupes (clusters) de phénomènes de sécurité », *Postal Mémorialis*, 2018, p. 165.
[87] J. TRULLEMANS, « Plan national de sécurité : Groupes (clusters) de phénomènes de sécurité », *op. cit.*, p. 166.
[88] J. TRULLEMANS, « Plan national de sécurité : Groupes (clusters) de phénomènes de sécurité », *op. cit.*, p. 166.
[89] B. COLFS et S. SMOOS, « Des caméras ANPR au service de l'apaisement des quartiers », *Mouvement communal*, août-septembre, 2023, p. 56.
[90] J. TRULLEMANS, « Evaluation de la loi du 10 avril 1990 réglementant la sécurité privée et particulière : Compétences générales et situationnelles », *op. cit.*, p. 129.
[91] X., « Histoire belge : les caméras intelligentes qui vont sanctionner le GSM au volant sont… illégales », RTL Info, 2022, https://www.rtl.be/actu/belgique/societe/histoire-belge-les-cameras-intelligentes-qui-vont-sanctionner-le-gsm-au-volant/2022-11-05/article/499617 (date de dernière consultation : 10 mars 2025).

automatiquement les conducteurs qui manipulent leur téléphone et, le cas échéant, de les sanctionner[92]. Cette proposition de loi vise à modifier et à étendre l'arrêté royal du 18 décembre 2002[93] qui délimite les infractions qui peuvent être constatées par des appareils fonctionnant automatiquement et sans la présence d'un agent qualifié avec une force probante particulière[94]. Lorsqu'une préparation de législation concerne le traitement de données à caractère personnel par les services de police intégrée, l'Organe de contrôle de l'information policière doit être préalablement consulté[95]. Ce dernier a alors rendu un avis et a mis en lumière l'illégalité qu'engendrait cette pratique, les lois régulant la reconnaissance faciale n'étant pas permissives[96]. En effet, il n'est pas permis de procéder à un traitement de données du conducteur qui permettrait une identification unique et, par conséquent, on ne saurait mettre en lien le comportement constaté avec le conducteur[97]. Cette proposition de loi n'a pas abouti sous l'ancienne législature. Cependant, l'accord de gouvernement 2025-2029 affirme vouloir mettre en place un cadre juridique, respectant toutes les règles applicables en matière de protection de la vie privée, permettant la détection de l'utilisation d'un téléphone au volant à l'aide d'un dispositif automatique et autonome[98].

c) Reconnaissance faciale

Comme exposé précédemment, le législateur n'a pas autorisé l'utilisation de la reconnaissance faciale et il n'existe pas en Belgique de cadre légal clair[99]. En effet, si la loi caméras affirme l'interdiction de tout autre caméra intelligente que celles dotées de la

[92] Proposition de loi modifiant l'arrêté royal du 18 décembre 2002 déterminant les infractions dont la constatation fondée sur des preuves matérielles fournies par des appareils fonctionnant automatiquement en l'absence d'un agent qualifié, fait foi jusqu'à preuve du contraire, en ce qui concerne l'usage du téléphone portable au volant, *Doc. parl.*, Ch. repr., sess. ord. 2020-2021, n°55-1722/001.

[93] A.R. du 18 décembre 2002 déterminant les infractions dont la constatation fondée sur des preuves matérielles fournies par des appareils fonctionnant automatiquement en l'absence d'un agent qualifié, fait foi jusqu'à preuve du contraire, art. 1er, *M.B.*, 25 décembre 2002, p. 58181.

[94] Organe de contrôle de l'information policière, « Avis relatif à la proposition de loi modifiant l'arrêté royal du 18 décembre 2002 en ce qui concerne l'usage du téléphone portable au volant », p. 3, https://www.organedecontrole.be/files/DA210003-FR.pdf (date de dernière consultation : 15 mars 2025).

[95] Organe de contrôle de l'information policière, « Avis relatif à la proposition de loi modifiant l'arrêté royal du 18 décembre 2002 en ce qui concerne l'usage du téléphone portable au volant », *op. cit*, p. 2.

[96] Organe de contrôle de l'information policière, « Avis relatif à la proposition de loi modifiant l'arrêté royal du 18 décembre 2002 en ce qui concerne l'usage du téléphone portable au volant », *op. cit.*, p. 2.

[97] Organe de contrôle de l'information policière, « Avis relatif à la proposition de loi modifiant l'arrêté royal du 18 décembre 2002 en ce qui concerne l'usage du téléphone portable au volant », *op. cit.*, p. 7.

[98] Accord de coalition fédérale 2025-2029, p. 109, https://www.belgium.be/sites/default/files/resources/publication/files/Accord_gouvernemental-Bart_De_Wever_fr.pdf (date de dernière consultation : 17 mars 2025).

[99] Ligue des droits humains, « 'On vous voit' : l'utilisation de la reconnaissance faciale et les questions de surveillance au centre du procès fictif de la Ligue des droits humains », 2024, https://www.liguedh.be/on-vous-voit-lutilisation-de-la-reconnaissance-faciale-et-les-questions-de-surveillance-au-centre-du-proces-fictif-de-la-ligue-des-droits-humains/ (date de dernière consultation : 17 mars 2025).

technologie ANPR, la loi sur la fonction de police, quant à elle, n'explicite pas le sort à réserver aux caméras de surveillance ayant pour finalité la reconnaissance faciale. Celle-ci est alors sujette à interprétation et il en résulte un flou juridique. L'article 20 de cette même loi précise la définition de caméra intelligente[100] et selon l'exposé des motifs, y inclus également les caméras permettant la reconnaissance faciale[101]. En revanche, elle ne dispose pas dans quelles circonstances ni sous quelles conditions l'utilisation de caméras permettant la reconnaissance faciale est autorisée, *a fortiori* elle n'organise pas l'enregistrement et la conservation des données recueillies[102]. En 2020, le ministre Philippe De Backer affirmait alors qu'aucune de ces deux lois n'autorisait l'utilisation de caméras à reconnaissance faciale et que par conséquent « il est interdit aux particuliers, mais aussi aux pouvoirs publics, de s'en servir »[103].

Cette absence de cadre juridique clair n'a pas freiné la police fédérale qui, au cours des dernières années, a eu recours à de maintes reprises à cette technologie[104]. Ces pratiques ont d'ailleurs donné lieu, en 2020, 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[105]. Celle-ci avait pour objectif d'interdire temporairement tout recours à la technologie de reconnaissance faciale afin que les droits fondamentaux des citoyens soient préservés le temps qu'une législation soit adoptée ; le moratoire ne portant pas sur une quelconque initiative législative[106].

---

[100] Loi du 5 août 1992, précitée, art. 25/2, §1er, 3°.

[101] 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, Exposés introductifs, *Doc. parl.*, Ch. repr., sess. ord. 2017-2018, n° 54 2855/003, p. 12 ; Organe de contrôle de l'information policière, « 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 à l'aéroport national de Zavente », p.4, https://www.organedecontrole.be/files/DIO19005_Contr%C3%B4le_LPABRUNAT_Reconnaissance_Faciale_Publique_F.PDF , (date de dernière consultation : 17 mars 2025), ci-après abrégé « Rapport intermédiaire ».

[102] Organe de contrôle de l'information policière, « Rapport intermédiaire », *op. cit.*, p. 4.

[103] 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. parl.*, Ch. repr., sess. ord. 2019-2020, n° 55-1349/001, p. 11.

[104] Ligue des droits humains, « 'On vous voit' : l'utilisation de la reconnaissance faciale et les questions de surveillance au centre du procès fictif de la Ligue des droits humains », *op. cit.*

[105] 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. parl.*, Ch. repr., sess. ord. 2019-2020, n° 55-1349/001, p. 11.

[106] Organe de contrôle de l'information policière, « 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 », 24 janvier 2022, https://www.organedecontrole.be/files/DA210029_Avis_F.pdf (date de dernière consultation le 16 mars 2025).

Les auteurs de cette résolution souhaitaient également qu'un débat sur ce sujet sensible soit mis en place « afin que cette technologie intrusive ne puisse être implémentée qu'accompagnée de garanties strictes concernant les droits humains »[107].

i. Aéroport national de Zaventem

En 2019, le commissaire général de la police fédérale déclarait lors d'une interview accordée à l'hebdomadaire flamand « Knack » que la technologie de reconnaissance faciale était utilisée à l'aéroport de Zaventem[108]. L'Organe de contrôle, responsable de la surveillance de la gestion de l'information policière ainsi qu'autorité de protection des données pour la police intégrée, n'ayant pas été informé d'un tel usage, a effectué une visite auprès de la police fédérale de l'aéroport de Zaventem et a rédigé consécutivement un rapport[109]. Il ressort de cette descente sur les lieux que le système dont il est sujet n'est plus qu'utilisé partiellement[110] . En effet, le logiciel a été acheté début 2017 mais au vu des nombreuses erreurs mises en lumière par les tests, notamment en raison de la couleur de peau des individus, du port de lunettes, de la pilosité, son usage a été interrompu[111]. Techniquement, il s'agit de quatre caméras créant des « snapshots », c'est-à-dire des modèles biométriques des personnes présentes sur les images vidéos, ces derniers sont enregistrés pour être ensuite comparés à des listes noires de création propre afin de potentiellement révéler une concordance[112].

L'enquête réalisée par l'Organe de contrôle met en lumière plusieurs irrégularités et en conséquence oblige l'Organe à prononcer une mesure corrective et à ordonner la suspension temporaire du système de reconnaissance faciale[113]. Bien qu'étant un projet considéré comme un projet pilote, l'Organe de contrôle insiste sur la nécessité pour ces expérimentations impliquant des données biométriques de respecter les mêmes garanties légales que toute autre utilisation[114]. Le commissaire général reconnait qu'une création d'une banque de données technique dans le cadre de la reconnaissance faciale n'est pas autorisée dans l'état actuel de la législation, l'article 44/2 de la loi sur la fonction de police prévoit uniquement une base de

[107] Organe de contrôle de l'information policière, « 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 », *op. cit.*
[108] Organe de contrôle de l'information policière, « Rapport intermédiaire », *op. cit.*, p. 3.
[109] Organe de contrôle de l'information policière, « Rapport intermédiaire », *op. cit.*, p. 3.
[110] Organe de contrôle de l'information policière, « Rapport intermédiaire », *op. cit.*, p. 3.
[111] Organe de contrôle de l'information policière, « Rapport intermédiaire », *op. cit.*, p. 3.
[112] Organe de contrôle de l'information policière, « Rapport intermédiaire », *op. cit.*, p. 3.
[113] B. PEETERS, « Het gebruik van camera's met gezichtsherkenning : perspectieven na het proefproject in Zaventem », *Politie & Recht*, 2020, p. 155.
[114] B. PEETERS, *op. cit.*, p. 159.

données que pour l'ANPR[115]. Celui-ci se défend et assure ne pas enfreindre la loi car en vertu de l'article 25/3 de la loi sur la fonction de police « le législateur a disposé qu'une caméra utilisée par les services de police, quel que soit son type, peut être équipée d'une technologie intelligente » et donc que « l'introduction d'une reconnaissance faciale en temps réel est donc à notre avis conforme à la loi »[116]. L'Organe conclut que l'usage de cette technologie ne possède pas, au jour de ces tests, de base légale suffisante encadrant les conditions d'utilisation et assurant le respect des droits fondamentaux des citoyens[117].

ii. Clearview

Clearview est une entreprise américaine qui a développé une application du même nom permettant à l'acheteur de comparer grâce à un logiciel de reconnaissance faciale des photos avec d'autres clichés stockés dans la banque de données de Clearview[118]. L'objectif de cette application est de venir en aide aux forces de police lors de leurs enquêtes en permettant une identification rapide des individus grâce à la base de données massivement fournie de Clearview[119]. Cette entreprise est sujette à débat et polémique car elle rassemble de manière importante des photos de sources numériques accessibles au public et les délivre, à des fins de profit, aux forces de l'ordre[120]. Le logiciel extrait les photos sur des pages web qui ne sont pas privées, notamment sur des sites judiciaires ainsi que sur les réseaux sociaux tels que Facebook, Twitter et Instagram, l'on nomme cette pratique « web scraping »[121].

À la suite d'articles parus dans les médias dénonçant l'utilisation de cette application par les services de police belges, l'Organe de contrôle de l'information policière a réalisé un rapport de contrôle[122]. Cette enquête fait apparaitre que deux membres de la police fédérale ont effectivement eu accès à une licence d'essai du programme et l'ont utilisé dans le cadre d'enquêtes sur de potentiels abus sexuels impliquant des mineurs[123]. Cela constitue un

[115] Loi du 5 août 1992, précitée, art. 44/2 ; B. PEETERS, *op. cit.*., p. 158.
[116] Loi du 5 août 1992, précitée, art. 25/3 ; Organe de contrôle de l'information policière, « Rapport intermédiaire », *op. cit.*, p. 4.
[117] B. PEETERS, *op. cit.*, p. 160.
[118] Organe de contrôle de l'information policière, « 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) », 2022, p. 4, https://www.organedecontrole.be/files/DIO21006_Rapport_Contrôle_Clearview_F_00050441.pdf (date de dernière consultation : 22 mars 2025).
[119] L. DROESBEKE, « Investigation : Clearview AI, quand la reconnaissance faciale porte atteinte à la vie privée », R.T.B.F., 13 juin 2023, https://www.rtbf.be/article/investigation-clearview-ai-quand-la-reconnaissance-faciale-porte-atteinte-a-la-vie-privee-11212380 (date de dernière consultation : 22 mars 2025).
[120] L. DROESBEKE, *op. cit.*
[121] L. DROESBEKE, *op. cit.*
[122] R. VANLEEUW, « Clearview AI : COC-rapport vernietigend voor Belgische Federale Politie », *Computerrecht*, 2022, p. 251.
[123] R. VANLEEUW, *op. cit.*, p. 251.

traitement de données biométriques menaçant gravement la vie privée, celui-ci doit respecter la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel ainsi que la loi du 5 août 1992 sur la fonction de police[124]. L'Organe de contrôle déclare que la loi sur la fonction de police ne permet pas d'avoir recours à cette forme de technologie de reconnaissance faciale et ajoute que le transfert d'informations et de données policières à caractère personnel à l'entreprise Clearview est un traitement de données illicite et illégitime[125]. En conséquence, il prononce trois recommandations et deux mesures correctrices, dont un avertissement stipulant que sera considéré comme illicite tout éventuel usage du dispositif de reconnaissance faciale de Clearview, d'une application similaire ou d'une banque de données jumelle ainsi que tout traitement de données à caractère personnel consécutif représentera une violation de la réglementation relative au traitement de données à caractère personnel[126].

Cette affaire est cependant à distinguer de l'usage de la reconnaissance faciale à l'aéroport de Zaventem exposé précédemment. Premièrement, le recours à la reconnaissance faciale est ciblé en ce qu'il n'est pas appliqué aux images de caméras installées dans les lieux publics mais bien aux photos dont la police est déjà en possession[127]. Ensuite, les photos en question ont été transmises à une entreprise commerciale ne faisant pas partie de l'ordre juridique de l'Union européenne, la police ne disposant pas du moindre contrôle sur la durée de conservation ou sur une éventuelle réutilisation commerciale de ces données biométriques[128].

L'utilisation de cette application n'a pas été condamnée qu'en Belgique. Les autorités de protection de la vie privée en Allemagne, en Italie et au Royaume-Uni ont également pris des décisions en ce sens[129]. Aux Pays-Bas, l'Autorité néerlandaise de protection des données a prononcé une amende administrative de 30,5 millions d'euros envers Clearview AI, ainsi que quatre astreintes obligeant la société à cesser ses infractions au RGPD[130]. En France, également

[124] Organe de contrôle de l'information policière, « 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) », *op. cit.*, p. 16.
[125] Organe de contrôle de l'information policière, « 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) », *op. cit.*, p. 17.
[126] Organe de contrôle de l'information policière, « 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) », *op. cit.*, p. 17.
[127] Organe de contrôle de l'information policière, « 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) », *op. cit.*, p. 12.
[128] R. VANLEEUW, *op. cit.*, p. 251.
[129] E. VAAL, « Boete voor Clearview AI », *Computerrecht*, 2024, p. 426.
[130] E. VAAL, *op. cit.*., p. 426.

pour les mêmes raisons, la CNIL a ordonné la cessation de toute activité de scraping et lui a infligé une amende de 20 millions d'euros[131].

iii. Briefcam

Briefcam est une entreprise israélienne détenue par Canon qui a mis au point un logiciel d'analyse pour images de vidéosurveillance, ce programme s'ajoute au système de vidéosurveillance en place[132]. L'entreprise présente le logiciel comme permettant « une maximisation de la valeur des investissements dans les systèmes de surveillance en rendant la vidéo consultable, exploitable et quantifiable » et en conséquence « une révision et une recherche rapides des vidéos, de la reconnaissance faciale, des alertes en temps réel et des analyses quantitatives des vidéos »[133]. Cette technologie, et plus particulièrement sa fonctionnalité de Vidéo Synopsis condensant plusieurs heures de vidéo en quelques minutes en regroupant les « objets », tels que les individus ou les véhicules, apparus à différents moments devant les caméras, attire la convoitise des policiers surchargés[134]. Le logiciel Briefcam est notamment utilisé par la police de la Région bruxelloise afin d'examiner, grâce à des algorithmes, les images des caméras qui filment l'espace public bruxellois[135]. La ville de Courtrai, en Flandre, est également friande de caméras de surveillance et s'intéresse de près à celles dites intelligentes[136]. Dans cette logique, la ville a fait appel à la société RTS afin d'y installer le logiciel Briefcam[137]. Comme mentionné, le logiciel dispose d'une option de reconnaissance faciale, celle-ci étant interdite en Belgique, la ville de Courtrai assure ne pas y avoir recours et que les droits d'utilisateurs ont été désactivés[138]. Néanmoins, la simple activation de cette fonction permettrait l'utilisation de la reconnaissance faciale par les services de police, l'obstacle à cette technologie n'est donc plus que législatif et non technique[139].

---

[131] P. SOENEN, S. PARSA et N. RAGHENO, « News », *DPO-pro mag*, 2023, p. 8.
[132] X., « Briefcam », Technopolice, https://technopolice.fr/briefcam/ (date de dernière consultation : 21 mars 2025).
[133] X. « What is video analytics », BriefCam, https://www.briefcam.com/technology/video-analytics/ (date de dernière consultation : 21 mars 2025).
[134] Q. NOIRFALISSE, « Courtrai, reconnaissance faciale dans le viseur ? », Médor, 23 décembre 2021, https://medor.coop/hypersurveillance-belgique-surveillance-privacy/police-justice-bng/episodes/courtrai-reconnaissance-faciale-dans-le-viseur-camera-criminalite-videosurveillance-briefcam-biometrie/?full=1 (date de dernière consultation : 25 mars 2025).
[135] C. DUBOIS, « Note d'analyse 9-24 du Centre d'études Jacques Georgin : Vers une législation de la reconnaissance faciale en Belgique ? Enjeux et stratégies », 20 septembre 2024, https://www.cejg.be/wp-content/uploads/2025/01/Note-danalyse-9-24-du-CeG-Enjeux-lies-au-deploiement-de-la-reconnaissance-faciale-en-Belgique.pdf (date de dernière consultation : 25 mars 2025).
[136] Q. NOIRFALISSE, *op. cit.*
[137] Q. NOIRFALISSE, *op. cit.*
[138] Q. NOIRFALISSE, *op. cit.*
[139] Q. NOIRFALISSE, *op. cit.*

Section 2 : Dans l'Union européenne

a) Jeux olympiques en France

Chez nos voisins français, les Jeux olympiques, ayant eu lieu cet été 2024, ont alimenté et accéléré davantage le débat quant à la reconnaissance faciale. Ces Jeux olympiques présentent une physionomie unique, ils prennent place dans un espace géographique étendu et durant une longue période de temps[140]. De plus, ils accueillent plus de 15 millions de spectateurs dans un niveau de menace certainement et particulièrement élevé[141].

Pour faire face à ces défis sécuritaires, le recours aux nouvelles technologies afin d'apporter un soutien efficace aux forces de sécurité et aux acteurs de la sécurité privée s'est naturellement présenté[142]. Pour ce faire un cadre juridique a été précisé quant à l'usage de la vidéo-augmentée, pour la première fois en France et en Europe[143]. En avril 2023, le Parlement français a approuvé la loi dite « olympique »[144]. Cette loi organise, de façon expérimentale, le recours à deux innovations technologiques : les scanners à ondes millimétriques et les caméras augmentées[145]. Plus précisément, le chapitre 3 de cette loi est consacré à cette expérimentation de la vidéosurveillance algorithmique[146]. L'objectif de ce dispositif est de générer des signalements lorsqu'une situation relevant du traitement de données survient, il analyse en temps réel des images et détecte des évènements préalablement désignés comme susceptibles de présenter ou de révéler un risque[147]. Ces évènements sont notamment des objets abandonnés, la présence ou l'utilisation d'armes, les mouvements de foule, le franchissement d'une ligne ou le simple fait de marcher à contresens[148]. Tout traitement algorithmique n'est cependant pas autorisé. Certains dispositifs de caméras augmentées sont proscrits. En effet, on y lit à l'article 10, une interdiction d'utilisation d'un système d'identification biométrique, d'une quelconque

---

[140] J. MERCIER, « Sécuriser les JOP 2024 : quelle place pour la technologie ? », *Annales des Mines – Enjeux numériques*, 2024, p. 14.
[141] J. MERCIER, *op. cit.*, p. 14.
[142] J. MERCIER, *op. cit.*, p. 15.
[143] J. MERCIER, *op. cit.*, p. 15.
[144] Loi n° 2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions ; J. DECROLY, « Les jeux olympiques de Paris 2024 : cheval de Troie de la vidéosurveillance algorithmique », *La Chronique de la Ligue des droits humains asbl*, 2024, n° 208, p. 14.
[145] J. MERCIER, *op. cit.*, p. 17.
[146] J. DECROLY, « Les jeux olympiques de Paris 2024 : cheval de Troie de la vidéosurveillance algorithmique », *op. cit.*, p. 14.
[147] A. GUILLARD et V. LOUIS, « La loi « jeux olympiques » : l'arbre de l'expérimentation algorithmique cache la forêt de l'extension sécuritaire », *La Revue des droits de l'homme*, 2023, p. 6.
[148] J. DECROLY, *Les jeux olympiques en valent-ils la chandelle ?*, Bruxelles, Editions de l'Université de Bruxelles, 2024, p. 185.

mise en œuvre d'une technique de reconnaissance faciale ou d'un processus d'interconnexion automatisée avec un traitement de données à caractère personnel[149].

L'association « La Quadrature du Net », militant contre la censure et la surveillance, alerte sur le véritable danger, postérieur aux Jeux olympiques[150]. En effet, cette phase expérimentale ouvrirait la porte aux entreprises présentes sur le marché, anticiperait et faciliterait le déploiement futur de la vidéosurveillance algorithmique[151]. Certaines dispositions de cette loi ont été applicables avant le début des Jeux olympiques et devaient le rester, initialement jusque mars 2025, tandis que la plupart des mesures ont une portée pouvant concerner tout rassemblement de personnes, s'intégrant ainsi à toute politique de maintien de l'ordre public[152]. La Ligue des droits humains alerte également sur le flou juridique et le manque de transparence de la loi « olympique »[153]. De plus, des utilisations hors cadre légal ont déjà été observées : des acteurs non repris dans la liste restrictive ont reçu l'autorisation par les services de police d'user de cette technologie[154].

Comme mentionné précédemment, cette expérimentation de la vidéo algorithmique devait prendre fin le 31 mars 2025. Le gouvernement a cependant souhaité prolonger ce dispositif pour deux années supplémentaires et a, pour ce faire, adopté un texte ce 18 mars 2025, malgré un appel du CNIL à voter contre cette mesure perfectionnant « un édifice de la surveillance qui transforme l'espace public en un espace de contrôle social permanent, qui trie les bons citoyens et les suspects »[155]. En réalité, cette prolongation a lieu dans le cadre d'une proposition de loi visant à renforcer la sûreté dans les transports[156]. Certains députés estiment que cela constitue un cavalier législatif, c'est-à-dire un amendement dans une loi en préparation qui ne présente pas de lien avec le texte en question, procédé condamnable par le Conseil

[149] Loi n° 2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions, art. 10, V.
[150] J. DECROLY, , *Les jeux olympiques en valent-ils la chandelle ?*, *op. cit.*, p. 185.
[151] J. DECROLY, *Les jeux olympiques en valent-ils la chandelle ?*, *op. cit.*,., p. 185.
[152] A. GUILLARD et V. LOUIS, *op. cit.*, p. 2.
[153] J. DECROLY, « Les jeux olympiques de Paris 2024 : cheval de Troie de la vidéosurveillance algorithmique », *op. cit*, p. 15.
[154] J. DECROLY, « Les jeux olympiques de Paris 2024 : cheval de Troie de la vidéosurveillance algorithmique », *op. cit.*, p. 15.
[155] La Quadrature du net, « VSA jusqu'en 2027 : quand le gouvernement ose tout », 7 février 2025, https://www.laquadrature.net/2025/02/07/vsa-jusquen-2027-quand-le-gouvernement-ose-tout/ (date de dernière consultation : 1er avril 2025).
[156] Amnesty International France, « Voici comment le gouvernement a prolongé la vidéosurveillance algorithmique », 2025, https://www.amnesty.fr/actualites/voici-comment-le-gouvernement-a-prolonge-la-videosurveillance-algorithmique (date de dernière consultation : 1er avril 2025).

constitutionnel[157]. Amnesty International attire l'attention sur le fait que cette prolongation suit pourtant un rapport d'évaluation peu convaincant[158]. Comme redouté et prédit, les Jeux olympiques ont joué un rôle catalyseur dans la normalisation des technologies de surveillance[159]. De surcroit, les responsables politiques ont manifesté leur intention d'étendre le champ de ces technologies, notamment à la reconnaissance faciale et ce dans toute la France[160].

b) Dans le reste de l'Europe

Ces technologies ne sont pas uniquement expérimentées en France. En effet, le nombre d'états membres de l'Union européenne réalisant des tests ou légiférant à ce sujet ne cesse de s'accroître.

A l'Est de l'Europe, la Hongrie n'est pas en reste quant à l'utilisation des technologies de reconnaissance faciale. En effet, ce pays, dirigé par Vicktor Orbán, est l'un des pionniers dans l'autorisation aux recours de technologies biométriques[161]. C'est une des raisons du conflit permanent entre les institutions de l'Union européenne et le pays au sujet de l'Etat de droit et plus particulièrement l'affaiblissement de l'indépendance judiciaire et des institutions démocratiques[162]. Le Parlement hongrois, en 2019, a adopté des lois afin de « simplifier et numériser certaines procédures » et, à cette occasion, la reconnaissance faciale à la fois judiciaire et en temps réel par la police a été légalisée[163] . Dorénavant, lorsqu'un individu ne peut fournir une pièce d'identité aux forces de l'ordre hongroises, celles-ci peuvent le prendre en photo et, grâce aux bases de données et à la reconnaissance faciale, l'identifier[164]. Cette opération n'est soumise à aucune autorisation judiciaire préalable[165].

---

[157] Amnesty International France, « Voici comment le gouvernement a prolongé la vidéosurveillance algorithmique », *op. cit.*
[158] Amnesty international France, « Voici comment le gouvernement a prolongé la vidéosurveillance algorithmique », *op. cit.*
[159] Amnesty International France, « Voici comment le gouvernement a prolongé la vidéosurveillance algorithmique », *op. cit.*
[160] Amnesty International France, « Voici comment le gouvernement a prolongé la vidéosurveillance algorithmique », *op. cit.*
[161] The Greens/EFA, « Biometric & behavioural mass surveillance in EU member states », p. 98 https://extranet.greens-efa.eu/public/media/file/1/7297 (date de dernière consultation : 21 mars 2025).
[162] The Greens/EFA, *op. cit.*, p. 98.
[163] The Greens/EFA, *op. cit.*, p. 98.
[164] The Greens/EFA, *op. cit.*, p. 98.
[165] The Greens/EFA, *op. cit.*, p. 98.

La police du Royaume-Uni a également pris part à l'examen des technologies de reconnaissance faciale en temps réel avec des listes de surveillance réelles[166]. Au Pays de Galles, les forces de l'ordre ont recours à ces avancées technologiques lors de grands évènements, notamment des manifestations sportives ou des concerts de musique[167]. En juin 2017, lors de la finale de la Ligue des champions de l'UEFA, ce dispositif a été mis en place et quatre listes de surveillance différentes ont été utilisées : « un petit nombre de personnes perçues comme présentant un risque sérieux pour la sécurité publique ; des personnes condamnées antérieurement pour des types d'infractions graves ; des personnes pouvant intéresser la police, dont la présence ne présentait pas de risque ou de menace immédiate pour la sécurité publique ; des images de policiers pour examiner l'efficacité du système »[168]. Peu d'informations sur le mode de création de ces listes ont été communiquées, cela complique l'appréciation de la finalité réelle, de la nécessité et du besoin social de l'utilisation de cette technologie[169]. Monsieur Bridge, citoyen anglais, s'est insurgé contre cette utilisation et a intenté une action en justice contre le chef de la police du sud du Pays de Galles, affirmant que ses données biométriques faciales avaient été capturées malgré lui et que ses droits fondamentaux dont son droit à la vie privée, à sa liberté d'expression et sa liberté de réunion avaient été violés[170]. La Cour d'appel n'a pas confirmé le jugement de première instance, elle a conclu que le manque de transparence et de définition du mode création des listes de surveillance, l'absence d'encadrement des lieux d'utilisation ainsi qu'une marge de discrétion trop étendue rendaient l'utilisation de cette technologie non conforme à la loi et violaient bel et bien l'article 8 de la CEDH[171].

En Allemagne, la police de Hambourg a utilisé le logiciel de reconnaissance faciale « Videmo 360 » afin d'analyser des images et vidéos dans le cadre des investigations menées en lien avec les infractions commises lors du sommet du G20 qui s'est tenu à Hambourg en juin

[166] F.R.A. « Technologie de reconnaissance faciale : considérations relatives aux droits fondamentaux dans le contexte de l'application de la loi », *Office des publications de l'Union européenne*, 2020, p. 12, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper_fr.pdf (date de dernière consultation : 21 mars 2025).
[167] F.R.A. « Technologie de reconnaissance faciale : considérations relatives aux droits fondamentaux dans le contexte de l'application de la loi », *op. cit.*, p. 12
[168] F.R.A. « Technologie de reconnaissance faciale : considérations relatives aux droits fondamentaux dans le contexte de l'application de la loi », *op. cit.*, p. 12
[169] F.R.A. « Technologie de reconnaissance faciale : considérations relatives aux droits fondamentaux dans le contexte de l'application de la loi », *op. cit.*, p. 12
[170] Appelate Court, R v. the Chief Constable of South Wales Police, 11 août 2020, C1:2019/2670.
[171] Appelate Court, R v. the Chief Constable of South Wales Police, 11 août 2020, C1:2019/2670.

2017[172]. La prolifération de ces projets pilotes habitue le citoyen à une surveillance en constance croissance, par exemple, les caméras installées à Hamburg à l'occasion du G20 sont toujours en place[173].

[172] Commissaire à la protection des données et à la liberté d'information de Hambourg, « Evaluation juridique en matière de protection des données de l'utilisation d'un logiciel de reconnaissance faciale par la police de Hambourg aux fins d'élucidation d'infractions en lien avec le sommet du G20 », 31 mai 2018, p. 2, https://datenschutz-hamburg.de/fileadmin/user_upload/HmbBfDI/Datenschutz/Informationen/Pruefbericht_Gesichtserkenungssoftware.pdf (date de dernière consultation : 3 mai 2025).
[173] The Greens/EFA, *op. cit.*, p. 96.

TITRE 2 : ENCADREMENT LEGISLATIF PAR L'UNION EUROPEENNE

"Aujourd'hui marque une étape majeure s'agissant du rôle de chef de file joué par l'Europe en matière d'IA digne de confiance. Grâce à l'entrée en vigueur du règlement sur l'IA, la démocratie européenne a mis en place un cadre efficace, proportionné et qui constitue une première mondiale en matière d'IA, en faisant face aux risques et en servant de plateforme pour les jeunes pousses européennes dans le domaine de l'IA." Thierry Breton, commissaire au marché intérieur - 01/08/2024 [174].

Chapitre 1 : Adoption AI Act

Section 1 : Historique des négociations

a) Etat législatif avant l'AI Act

Antérieurement au règlement européen sur l'intelligence artificielle, le cadre juridique concernant la reconnaissance faciale couvrait uniquement la régulation du traitement des données. Ces nouvelles technologies de surveillance de masse recueillent des données à caractère personnel, les stockent et les traitent. Cela implique que, généralement sur le plan du droit national et assurément sur le plan du droit de l'Union européenne, les personnes faisant l'objet de ce traitement y aient consenti[175]. Nous trouvons des pistes de dispositions applicables à la surveillance biométrique dans les espaces publics au sein de la législation secondaire de l'Union européenne et plus particulièrement dans le règlement général sur la protection des données et dans la directive relative à la protection des données dans le domaine répressif [176]. Le RGPD légifère de façon plus générale, il établit des règles concernant le traitement des données personnelles pour quasiment toutes les finalités[177]. Cependant, en vertu de l'article 2, §2, d), de ce même règlement, celui-ci ne s'applique notamment pas lorsque le traitement est effectué « 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, y compris la protection contre des menaces pour la sécurité publique et la prévention de telles

[174] Commission européenne, « Communiqué de presse : Entrée en vigueur du règlement européen sur l'intelligence artificielle », 1er août 2024, https://ec.europa.eu/commission/presscorner/api/files/document/print/fr/ip_24_4123/IP_24_4123_FR.pdf (date de dernière consultation : 24 mars 2025).
[175] S. PEYROU, « Nouvelles technologies, sécurité et protection des données à caractère personnel : un cadre juridique européen à la hauteur des enjeux ? », *Cahiers de la sécurité et de la justice*, 2022, p. 189.
[176] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, précité ; Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016, précitée.
[177] The Greens/EFA, *op. cit.*, p. 50.

menaces »[178]. La législation applicable, lorsque ces finalités sont rencontrées, est la directive relative à la protection des données dans le domaine répressif, appelée directive « justice-police » ou encore « LED »[179]. Nous pouvons et nous devons également nous référer au droit primaire qui garantit notamment les droits fondamentaux. Au sein du Titre 3 de ce travail, nous les analysons plus amplement.

Ces données personnelles peuvent être qualifiées de « sensibles », en ce qu'elles révèlent « l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses, philosophiques, l'appartenance syndicale, les informations concernant la santé, la vie sexuelle ou l'orientation sexuelle d'une personne physique » et, ce qui nous intéresse d'autant plus dans ce travail, « les données biométriques aux fins d'identifier une personne de manière unique »[180].

Des dispositions spécifiques sont alors prévues pour ces données sensibles, dont les données biométriques font partie. Ces données biométriques sont définies de façon identique par le règlement et par la directive comme « les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractères physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques »[181]. De plus, pour être qualifiées de données biométriques et bénéficier d'une protection plus élevée les données personnelles doivent remplir deux conditions. Premièrement, elles doivent faire l'objet d'un traitement spécifique et, secondement, permettre l'identification directe et unique d'un individu[182].

L'article 9 du règlement général de protection des données interdit leur traitement sauf strictes exceptions[183]. Nous concentrons notre attention sur l'encadrement légal instauré par la directive police-justice, applicable à la surveillance biométrique à des fins répressives dans les espaces publics, les normes du règlement général de protection des données ne s'appliquant pas aux traitements à des fins de maintien de l'ordre[184]. L'article 10 de la directive police-justice

[178] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, précité, art. 2, §2, d).
[179] Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016, précitée, art. 2.
[180] J.-F. RENUCCI et A. RENUCCI, *Droit et protection des données à caractère personnel, droit européen : RGPD, Convention européenne des droits de l'homme*, Paris, LGDJ, 2022, p. 197.
[181] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, précité, art. 4, (14) ; Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016, précitée, art. 3, (13).
[182]The Greens/EFA, *op. cit.*, p. 51.
[183] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, précité, art. 9 ; A. CAYOL, « La protection des données personnelles de santé en France et en Europe par le Règlement Général sur la Protection des Données (RGPD) », *Droit, Santé et Société*, 2021, p. 53.
[184] Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016, précitée, art. 1er, §1er ; The Greens/EFA, *op. cit.*, p. 51.

n'autorise le traitement portant sur ces catégories particulières de données à caractère personnel que si la situation présente une nécessité absolue, que des garanties appropriées pour les droits et libertés de la personne concernée sont assurées et que nous nous trouvons dans une des trois hypothèses limitativement listées[185]. Ces hypothèses de traitement sont au nombre de trois : « a) lorsqu'ils sont autorisés par le droit de l'Union ou le droit d'un état membre ; b) pour protéger les intérêts vitaux de la personne concernée ou d'une autre personne physique ; ou c) lorsque le traitement porte sur des données manifestement rendues publiques par la personne concernée »[186].

b) Jurisprudence

Les cours et tribunaux se sont également exprimés, de façon plus générale, sur l'utilisation des technologies dans le domaine de la sécurité, en raison de la surveillance de masse et de l'intrusion dans la vie privée des citoyens qu'elles engendrent. La reconnaissance faciale, et c'est notamment ce qui lui est reproché, contribue à ce suivi systématique de la population. Ces arrêts nous éclairent alors sur la position des instances européennes concernant le sujet. Initialement réfractaire, la tendance semble s'inverser[187].

La reconnaissance faciale entraine le recueil et la conservation des données personnelles des individus. Dans un premier temps, plusieurs arrêts ont condamné cette pratique. La Cour de justice de l'Union européenne, dans l'affaire *Digital Rights Ireland*, a estimé que le devoir contraint aux fournisseurs de communications électroniques de conserver les métadonnées de communication, visant à garantir leur disponibilité aux autorités publiques, constituait une ingérence, d'une vaste ampleur et particulièrement grave, dans les droits au respect de la vie privée et à la protection des données à caractère personnel, garantis par les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne[188]. De fait, cette obligation de sauvegarde de masse de données généralisée, indifférenciée, dont l'accès n'était encadré que de manière lacunaire, ne prévoyant pas les conditions matérielles et procédurales d'accès des autorités nationales compétentes aux données concernées, ressort initialement de la directive européenne 2006/24/CE qui a alors été invalidée[189].

---

[185] Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016, précitée, art. 10 ; J.-F. RENUCCI et A. RENUCCI, *op. cit.*, p. 197.
[186] Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016, précitée, art. 10.
[187] S. PEYROU, *op. cit.*, p. 192.
[188] C. DE TERWAGNE, « L'illégalité nuancée de la surveillance numérique : la réponse des juridictions belges et française à l'arrêt *La Quadrature du Net* de la Cour de justice de l'Union européenne », *Rev. Trim. D. H.*, 2022, p. 4.
[189] C. DE TERWAGNE, *op. cit.*, p. 4.

Les années suivantes, l'arrêt *Schrems* ainsi que l'arrêt *Tele2 Sverige* sont venus confirmer ce verdict d'ingérence dans la vie privée[190]. La Cour réitère sa condamnation quant au traitement systématique et non ciblé des données relatives au trafic et des données de localisation mais l'admet également dans de strictes hypothèses[191]. A la lumière de ces arrêts, la reconnaissance faciale, étant donné qu'elle effectue une surveillance de masse de manière généralisée et indifférenciée, parait incompatible avec la jurisprudence de la Cour de justice[192].

Dans un second temps, la Cour de justice a paru adopter une position plus modérée et cautionner, dans une certaine mesure, la surveillance de masse. Elle a notamment conclu, dans l'avis 1/15 concernant l'accord PNR UE-Canada permettant aux autorités compétentes de recueillir et de traiter les données des dossiers des passagers aériens, que la lutte contre le terrorisme et la criminalité transnationale grave « était susceptible de justifier des ingérences, même graves, dans les droits fondamentaux »[193]. Nous observons le même constat dans son arrêt *Privacy International*[194]. Bien que réaffirmant fermement son opposition à la transmission et la conservation généralisée et indifférenciée de données relatives au trafic et à la localisation, elle reconnait une dérogation significative à l'obligation de garantir la confidentialité des données, lorsqu'un état membre rencontre « une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible », comme une menace d'attentat terroriste par exemple[195]. Nous pouvons établir un lien avec la réglementation de la reconnaissance faciale, puisque le même type de situation de crise justifie et autorise, dans une certaine mesure, son utilisation.

Le juge de la Cour européenne des droits de l'homme partage la nouvelle position de la Cour de justice de l'Union européenne[196]. En effet, dans son récent arrêt *Big Brother Watch*[197] elle admet un droit aux états membres à la surveillance de masse des communications électroniques dans le cadre de la préservation de la sécurité nationale, sous réserve d'une garantie de transparence du traitement des données et d'un accès à un recours effectif[198].

---

[190] C.J.U.E. (gde ch.), S*chrems c. Data Protection Commissioner*, C-362/14, ECLI:EU:C:2015:650 ; C.J.U.E. (gde ch.), *Tele2 Sverige AB c. Post-och telestyrelsen*, C-203/15, ECLI:EU:C:2016:970.
[191] C. DE TERWAGNE, *op. cit.*, p. 5.
[192] S. PEYROU, *op. cit.*, p. 194.
[193] S. PEYROU, *op. cit.*., p. 194.
[194] C.J.U.E. (gde ch.), *Privacy International c. Secretary of State for Foreign and Commonwealth Affairs e.a.*, C-623/17, ECLI:EU:2020:790.
[195] S. PEYROU, *op. cit*., p. 195.
[196] S. PARSA et E. VOLCANSEK, « L'impact de la protection des données sur la surveillance de masse : examen de l'arrêt Big Brother Watch et autres c. Royaume-Uni de la Cour européenne des droits de l'homme », *DPO news*, 2022, pp. 8-13.
[197] Cour eur. dr. h. (gde ch.), arrêt Big Brother Watch c. Royaume-Uni du 25 mai 2021.
[198] S. PARSA et E. VOLCANSEK, *op. cit.*, pp. 8-13.

La Cour soutient fermement que les Etats disposent d'une large marge d'appréciation dans le choix des moyens voués à assurer leur sécurité nationale[199]. A fortiori, elle déclare qu'à la lecture de l'article 8 de la Convention européenne des droits de l'homme, on ne peut déduire une interdiction du recours à l'interception en masse afin de protéger la sécurité nationale ou d'autres intérêts nationaux essentiels contre des menaces extérieures graves, bien que celle-ci doive, assurément et tout au long de l'opération, répondre aux garanties de nécessité et proportionnalité[200].

La Cour européenne des droits de l'homme s'est prononcée à titre inaugural, le 4 juillet 2023, précisément sur la question de l'usage de la reconnaissance faciale à des fins répressives[201]. L'affaire oppose Monsieur Glukhin contre la Russie.

Voici un bref exposé des faits : Monsieur Glukhin a emprunté, seul, le métro de Moscou, muni d'une silhouette en carton grandeur nature d'un célèbre activiste et d'un écriteau « Je risque jusqu'à 5 ans de prison pour des manifestations pacifistes »[202]. Cette action a été considérée par les autorités russes comme une manifestation illicite, n'ayant pas été notifiée au préalable[203]. Peu de temps après, Monsieur Glukhin a été arrêté dans le métro. Ce dernier suspecte que les autorités ont usé de technologies de reconnaissance faciale afin de l'identifier et de le retrouver dans la ville. La Cour suit le requérant dans son raisonnement et estime que les articles 8 et 10 de la Convention européenne des droits de l'homme sont violés[204]. Elle déclare qu'il a fait l'objet d'un traitement de ses données à caractère personnel excessivement intrusif et qu'*in casu* « le recours à la technologie de reconnaissance faciale a été incompatible avec les idéaux et valeurs d'une société démocratique »[205].

Il est important de noter que cette sentence n'établit cependant pas une condamnation pure et simple de principe, du procédé de reconnaissance faciale[206]. En effet, la Cour, afin d'évaluer l'ingérence, a effectué l'habituel triple test de prévisibilité, légitimité et

---

[199] F. DUBUISSON, « La Cour européenne des droits de l'homme face à la surveillance de masse », obs. sous Cour eur. dr. h. (gde ch.), arrêt Big Brother Watch c. Royaume-Uni du 25 mai 2021, *Rev. trim. D. H.*, 2022, p. 129.
[200] S. PEYROU, *op. cit*., p. 195
[201] F. COTON, « Reconnaissance faciale dans l'espace public à des fins répressives : la CEDH ne condamne pas le principe, le Règlement IA l'encadre », *R.D.T.I.*, 2024, p. 185 ; Cour eur. dr. h., arrêt Glukhin c. Russie du 4 juillet 2023.
[202] J.-P. MARGUENAUD et D. ROETS, « Droits de l'homme : jurisprudence de la CEDH », *Revue de science criminelle et de droit pénal comparé*, 2023, p. 630.
[203] F. COTON, *op. cit.*, p. 186.
[204] D. SZYMCZAK, « Chronique de jurisprudence de la Cour européenne des droits de l'homme (2023) », *Rev. trim. D. H.*, 2024, p. 378.
[205] D. SZYMCZAK, *op. cit.*, p. 378.
[206] F. COTON, *op. cit.*, p. 187.

proportionnalité de la norme nationale sur laquelle les autorités répressives russes appuient leur action[207].

c) Chronologie

En avril 2021, la Commission a déposé une proposition de règlement sur l'intelligence artificielle[208]. Cette proposition fait suite aux réquisitions explicites du Parlement européen ainsi que du Conseil européen de légiférer en la matière[209]. En effet, déjà en 2017, ils clamaient le besoin de faire preuve « d'un sens de l'urgence face aux questions de l'intelligence artificielle »[210]. De plus, Madame Ursula von der Leyen, dans ses orientations politiques pour la Commission 2019-2024 nommées « Une Union plus ambitieuse », soutenait cette démarche et assurait que durant ses 100 premiers jours de mandat « une proposition législative en vue d'une approche européenne coordonnée relative aux implications humaines et éthiques de l'intelligence artificielle » serait présentée[211].

Après plusieurs amendements et discussions, la loi sur l'intelligence artificielle, approuvée par le Parlement et le Conseil, a fait l'objet d'une publication au Journal officiel de l'Union européenne le 12 juillet 2024[212]. Cette procédure législative aura alors duré un peu plus de trois années.

Le choix d'un règlement en tant qu'instrument juridique par l'Union européenne n'est pas anodin et va de pair avec l'objectif de l'Union européenne de renforcer la sécurité juridique concernant le développement et l'utilisation de l'intelligence artificielle. En vertu de l'article 288 T.F.U.E., un règlement a une portée générale, il est obligatoire dans tous ses éléments et est directement applicable dans tous les états membres de l'Union européenne[213], réduisant ainsi la

[207] F. COTON, *op. cit.*, p. 187.
[208] 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) 206 final, 21 avril 2021.
[209] Proposition de règlement (UE) 2021/0106 du Parlement européen et du Conseil du 24 avril 2021, précitée.
[210] Proposition de règlement (UE) 2021/0106 du Parlement européen et du Conseil du 24 avril 2021, précitée ; Conseil européen, « Réunion du Conseil européen (19 octobre 2017) – Conclusions, EUCO 14/17 », 2017, p. 7, https://data.consilium.europa.eu/doc/document/ST-14-2017-INIT/fr/pdf, (date de dernière consultation : 26 mars 2025).
[211] U. Von Der Leyen « Une Union plus ambitieuse, Mon programme pour l'Europe : orientations politiques pour la prochaine commission européenne 2019-2024», https://commission.europa.eu/document/download/063d44e9-04ed-4033-acf9-639ecb187e87_fr?filename=political-guidelines-next-commission_fr.pdf (date de dernière consultation : 27 mars 2025).
[212] H. POUGET, « Contexte institutionnel », Future of Life Institute, https://artificialintelligenceact.eu/fr/contexte/ (date de dernière consultation : 29 mars 2025) ; X., « Chronologie historique », Future of Life Institute, https://artificialintelligenceact.eu/fr/developpements/ (date de dernière consultation : 29 mars 2025).
[213] T.F.U.E., art. 288.

fragmentation juridique et simplifiant la mise en place d'un marché unique pour des systèmes d'IA licites, sûrs et dignes de confiance[214].

Section 2 : Finalités

En 2021, la Commission énonçait, dans sa proposition de cadre réglementaire relatif à l'intelligence artificielle, les quatre objectifs spécifiques suivants :

- « Veiller à ce que les systèmes d'IA mis sur le marché de l'Union et utilisés soient sûrs et respectent la législation en vigueur en matière de droits fondamentaux et les valeurs de l'Union ;
- garantir la sécurité juridique pour faciliter les investissements et l'innovation dans le domaine de l'IA ;
- renforcer la gouvernance et l'application effective de la législation existante en matière de droits fondamentaux et des exigences de sécurité applicables aux systèmes d'IA ;
- faciliter le développement d'un marché unique pour des applications d'IA légales, sûres et dignes de confiance, et empêcher la fragmentation du marché »[215].

Ce règlement a pour vocation de s'adapter à l'évolution des systèmes d'intelligence artificielle. Cela implique qu'elle fournisse une définition uniforme et neutre sur le plan technologique[216]. Comme nous l'explique le considérant 5 de l'AI Act, les intérêts publics et les droits fondamentaux protégés par le droit de l'Union doivent être préservés. Pour cela une législation adaptée et adéquate est nécessaire[217].

Les développeurs, comme les utilisateurs, doivent pouvoir bénéficier d'une sécurité juridique[218]. La sécurité juridique est reconnue comme un principe général du droit dans l'ordre de l'Union européenne[219]. La Cour de justice énonce dans un arrêt de 1990 que « tout acte doit être clair et précis afin que les justiciables puissent identifier leurs droits et obligations et adapter

[214] Proposition de règlement (UE) 2021/0106 du Parlement européen et du Conseil du 24 avril 2021, précitée.
[215] Proposition de règlement (UE) 2021/0106 du Parlement européen et du Conseil du 24 avril 2021, précitée.
[216] Parlement européen, « Loi sur l'IA de l'UE : première réglementation de l'intelligence artificielle », 27 mars 2024, https://www.europarl.europa.eu/ (date de dernière consultation : 28 mars 2025).
[217] Proposition de règlement (UE) 2021/0106 du Parlement européen et du Conseil du 24 avril 2021, précitée.
[218] S. FODOR, « Un cadre juridique pour une intelligence artificielle éthique : le règlement IA », *I2D – Information, données et documents*, 2024, p. 79.
[219] G. VALDELIEVRE, "La sécurité juridique – Le point de vue de l'avocat », *Titre VII*, 2020/2, p. 13.

leur comportement en conséquence »[220]. Elle ne peut être obtenue par des solutions nationales qui ne feraient que compliquer l'adoption de l'intelligence artificielle sur le marché[221].

La législation européenne sur les droits fondamentaux tels que la protection des données, le respect de la vie privée, la non-discrimination, ainsi que les normes sur la protection des consommateurs, sur la sécurité des produits et la responsabilité du fait des produits s'applique aux développeurs d'intelligence artificielle[222]. Cependant, les particularités de l'intelligence artificielle nécessitent une législation adéquate[223]. L'AI Act ambitionne d'apporter une législation commune à l'ensemble des secteurs, sauf le secteur militaire, portant sur la fabrication, le développement et l'usage de tout type d'IA afin de combler le vide juridique[224].

L'Union européenne, à travers l'AI Act, tente de promouvoir l'innovation des systèmes d'intelligence artificielle tout en veillant à la sauvegarde des intérêts et des droits des particuliers, des consommateurs. Particulièrement, compte tenu des règles spécifiques sur la protection des personnes physiques à l'égard du traitement des données à caractère personnel, concernant les restrictions à l'utilisation de systèmes d'IA pour l'identification biométrique à distance à des fins répressives, à l'utilisation de systèmes d'IA pour l'évaluation des risques des personnes physiques à des fins répressives et à l'utilisation de systèmes d'IA pour la catégorisation biométrique à des fins répressives[225], elle tente d'atteindre un certain équilibre entre un bon fonctionnement du marché intérieur, soutenu par les articles 26 et 114 T.F.U.E., et une protection des données personnelles optimale assurée par l'article 16 T.F.U.E.[226].

Les premiers considérants de ce règlement affirment fermement cette poursuite de justesse et d'harmonie. De fait, le premier considérant dispose que le règlement « garantit la

---

[220] C.J.U.E. (troisième ch.), *Vandemoortele c. Commission*, C-172/89, ECLI :UE :C :1990 :457 ; G. VALDELIEVRE, *op. cit.*, p. 13.
[221] Proposition de règlement (UE) 2021/0106 du Parlement européen et du Conseil du 24 avril 2021, précitée.
[222] Commission européenne, « Livre blanc : Intelligence artificielle, une approche européenne axée sur l'excellence et la confiance », COM/2020/65 final, p. 11, https://www.europarl.europa.eu/ (date de dernière consultation : 28 mars 2025).
[223] Commission européenne, « Livre blanc : Intelligence artificielle, une approche européenne axée sur l'excellence et la confiance », *op. cit.*, p. 11.
[224] K. DESVEAUD, *L'intelligence artificielle décryptée : Comprendre les enjeux et les risques éthiques de l'IA pour mieux l'appréhender*, Caen, EMS Editions, 2024, p. 225.
[225] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024, établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 202/1828, *J.O.U.E.*, 12 juillet 2024, série L, cons. 3.
[226] T.F.U.E., art. 16, 26 et 114 ; B. BERTRAND, « La politique de l'Union européenne en matière d'intelligence artificielle : entre approche sectorielle et transversale » *in Un droit de l'intelligence artificielle : entre règles sectorielles et régime général* (sous la dir. de C. CASTETS et J. EYNARD), Bruxelles, Bruylant, 2023, p. 75.

libre circulation transfrontalière des biens et services fondés sur l'intelligence artificielle, empêchant ainsi les états membres d'imposer des restrictions au développement, à la commercialisation et à l'utilisation des systèmes d'IA, à moins que le présent règlement ne l'autorise explicitement »[227].

En ce sens, en son titre 6 « Mesures de soutien à l'innovation », il instaure notamment une obligation, pour les autorités compétentes des états membres, de créer des bacs à sable réglementaires[228], « des environnements de test dans lesquels les entreprises peuvent contrôler leurs produits et leurs innovations sans ressentir le plein pouvoir de l'appareil de régulation étatique »[229].

Chapitre 2 : Contenu AI Act

Section 1 : Généralités

L'AI Act est le premier règlement encadrant l'utilisation de l'intelligence artificielle ainsi que son marché émergent[230]. De manière générale, ce règlement s'applique quel que soit le type d'activité pour lequel les systèmes d'intelligence artificielle sont développés et utilisés, que ce soit par des entreprises ou des personnes de droit privé, ainsi que par les autorités publiques et les administrations[231]. Nous y retrouvons 12 chapitres principaux. Ce texte est perçu comme compliqué et technique, il ne comporte pas moins de 180 considérants, 113 articles, 68 définitions et 13 annexes[232]. De plus, il doit être interprété à la lumière d'autres règlements et directives européennes en matière de données comme la DSA, DMA, DGA, Data Act, ainsi qu'en parallèle de nombreuses lignes directrices[233].

Le premier chapitre reprend les dispositions générales telles que l'objet, le champ d'application et des définitions. Le règlement fait référence à d'autres textes législatifs de l'Union européenne, notamment lorsqu'il s'agit de définitions. Nous retrouvons, au sein de l'article 3 de l'AI Act, de nombreuses définitions dont celle de « données biométriques »[234].

---

[227] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024, précité, cons. 1er.
[228] B. BERTRAND, *op. cit.*, p. 91.
[229] M. TRSTENJAK, « Analyse des bas à sable réglementaires d'IA dans l'AI Act », *R.P.I.N.*, 2024/19, p. 12.
[230] M. TRSTENJAK, *op. cit.*, p. 11.
[231] B. DOCQUIR, « Dompter les algorithmes ? Le nouveau règlement européen sur l'intelligence artificielle », *in Les platefromes numériques et l'intelligence artificielle* (sous la dir. de B. DOCQUIR), Limal, Anthemis, 2024, p. 243.
[232] A. BEELEN, « RGPD et intelligence artificielle : ce qu'il faut savoir du nouveau règlement européen », *D.P.O. News*, 2025, p. 12.
[233] A. BEELEN, *op.cit.*, p. 12.
[234] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024, précité, art. 3, 34°.

Cette définition est équivalente à celles établies par le règlement général de protection des données et par la directive police-justice. Le considérant 14 dispose en ce sens, que cette définition doit être interprétée à l'aune de ces dispositions précitées[235]. Une définition incontournable est celle de système d'intelligence artificielle, le règlement arrête cette notion en tant que « système automatisé qui est conçu pour fonctionner à différents niveaux d'autonomie et peut faire preuve d'une capacité d'adaptation après son déploiement, et qui, pour des objectifs explicites ou implicites, déduit, à partir des entrées qu'il reçoit, la manière de générer des sorties telles que des prédictions, du contenu, des recommandations ou des décisions qui peuvent influencer les environnements physiques ou virtuels »[236].

Le dernier article de ce premier chapitre prône une maîtrise de l'IA, explicitée dans le considérant 20, une éducation à l'IA devant permettre « aux fournisseurs, aux déployeurs et aux personnes concernées d'acquérir les notions nécessaires pour prendre des décisions éclairées en ce qui concerne les systèmes d'IA et d'en tirer ainsi le meilleur tout en protégeant les droits fondamentaux, la santé, la sécurité et de permettre un contrôle démocratique »[237].

Le règlement organise également l'application et le respect des règles qu'il établit. Des autorités nationales, ayant pour mission de superviser l'application des règles et exerçant des activités de surveillance du marché, doivent être nommées par les états membres, et ce avant le 2 août 2025[238]. De plus, un Bureau de l'IA est institué au sein de la Commission européenne et constitue l'organe central chargé de la mise en œuvre du règlement à l'échelle de l'Union. Il assure également la supervision du respect des règles applicables aux modèles d'IA à usage général[239]. Des organes consultatifs sont également créés : un Comité européen de l'intelligence artificielle, un groupe scientifique composé d'experts indépendants ainsi qu'un forum consultatif[240]. Le chapitre 12 établit des sanctions et des amendes en cas de non-respect des dispositions du présent règlement.

L'article 113 du règlement organise son entrée en vigueur[241]. Bien que le règlement soit entré en vigueur au jour du 1er août 2024, aucune disposition de la loi ne s'applique directement.

---

[235] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024, précité, cons. 14.
[236] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024, précité, art. 3.
[237] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024, précité, cons. 20 et art. 4.
[238] Commission européenne, « Communiqué de presse : Entrée en vigueur du règlement européen sur l'intelligence artificielle », *op. cit.*
[239] Commission européenne, « Communiqué de presse : Entrée en vigueur du règlement européen sur l'intelligence artificielle », *op. cit.*
[240] Commission européenne, « Communiqué de presse : Entrée en vigueur du règlement européen sur l'intelligence artificielle », *op. cit.*
[241] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024, précité, art. 113.

Cet article dispose que le règlement prend effet à partir du 2 août 2026 mais il établit néanmoins des exceptions avançant l'applicabilité de certaines dispositions ou au contraire les postposant. Les chapitres 1 et 2, reprenant les dispositions générales et établissant les pratiques interdites en matière d'intelligence artificielle, s'appliquent déjà, quant à eux, depuis le 2 février 2025[242].

Section 2 : Le risque, critère de régulation

Le règlement européen sur l'intelligence artificielle a fait le choix d'une approche fondée sur le risque, en évaluant le potentiel danger que représente un système d'intelligence artificielle pour la sécurité humaine et les droits fondamentaux[243]. En choisissant comme critère l'appréciation du risque, cette législation pourra s'adapter aux innovations[244]. L'objectif est que ce cadre juridique ne tombe pas en désuétude à la moindre avancée technologique[245].

Il existe quatre niveaux de risque. En fonction du degré dans lequel le système d'intelligence artificielle se situe, les exigences qui pèseront sur celui-ci seront proportionnellement différentes, le régime est plus souple pour les systèmes d'intelligence artificielle présentant des risques minimes[246].

Le niveau de risque le plus bas, appelé minimal, n'est pas régulé par le règlement car il n'implique aucun danger significatif, il couvre la plupart des applications d'intelligence artificielle que l'on retrouve sur le marché, comme les jeux vidéo incluant cette technologie[247]. La doctrine reconnait cette catégorie comme résiduelle[248]. Un grade au-dessus, nous retrouvons les systèmes nécessitant des garanties de transparence[249]. En vertu de l'article 50 du règlement[250], les fournisseurs et les déployeurs de systèmes d'intelligence artificielle destinés à interagir directement avec des personnes physiques doivent s'assurer que les utilisateurs finaux sont conscients d'être en interaction avec une intelligence artificielle[251].

Les deux derniers niveaux nous intéressent davantage en ce qu'ils concernent des systèmes pouvant fortement porter atteinte aux droits fondamentaux. Le chapitre 3 établit des

---

[242] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024, précité, art. 113, a).
[243] M. NUYTTEN, « De Europese Commissie onthult een nieuwe reeks voorstellen om artificiële intelligentie te reguleren», *T.B.H.*, 2021/5, p. 662.
[244] S. FODOR, *op. cit.*, p. 81.
[245] S. FODOR, *op. cit.*, p. 81.
[246] V. VERDOODT, "The regulation of artificial intelligence", *in An Introduction to Law & Technology* (sous la dir. de E. Lievens, C. Vander Maelen et S. Verschaeve), Gand, Owl Press Legal, 2024, p. 432.
[247] X. « High level summary of the AI Act", Future of Life Institute, 27 février 2024, https://artificialintelligenceact.eu/high-level-summary/ (date de dernière consultation : 30 mars 2025).
[248] A. BEELEN, *op. cit.*, p. 13.
[249] A. BEELEN, *op. cit.*, p. 13.
[250] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024, précité, art. 50.
[251] X. « High level summary of the AI Act", *op. cit.*

obligations strictes pour les systèmes à haut risque, représentant une part importante du règlement, tandis que le chapitre 2 reprend et explique les systèmes purement et simplement interdits[252]. Les systèmes interdits par le chapitre 2 sont notamment les systèmes de « social scoring », évaluant et catégorisant les individus en fonction de leur comportement social ou de certaines de leurs caractéristiques et influençant le traitement dont ils font l'objet[253]. À l'image du crédit social en Chine, les individus appartiennent à une liste assortie d'incitations et de sanctions, afin de les encourager à être, aux yeux du gouvernement, de meilleurs citoyens[254]. Les systèmes usant de techniques manipulatrices et trompeuses dans le but d'influencer les comportements d'une personne, exploitant ses vulnérabilités , et de réduire la capacité de prise de décision éclairée menant à un dommage d'ordre physique ou psychologique sont également proscrits[255].

Un dernier régime est instauré, régulant les modèles d'intelligence artificielle dits à « usage général » couvrant les modèles hautement performants qui permettent de réaliser un large panel d'activités, comme la rédaction d'un texte semblable à celle d'un humain[256]. Le règlement leur impose une garantie de constance transparence et prévoit des remèdes quant aux risques systémiques de ces modèles les plus performants[257].

Section 3 : Quant aux systèmes d'identification biométrique

a) Technologies biométriques

À la lecture du règlement, nous remarquons qu'il n'est pas uniquement question d'identification biométrique mais que trois types de système d'intelligence artificielle impliquant tous la biométrie sont définis différemment : l'identification biométrique à distance, la catégorisation biométrique et les systèmes de reconnaissance des émotions.

L'identification biométrique à distance ne doit pas se confondre avec la vérification biométrique. Cette dernière est définie comme « la vérification 'un à un' automatisée, y compris l'authentification, de l'identité des personnes physiques en comparant leurs données

[252] A. BEELEN, *op. cit.*, p. 13.
[253] X. « High level summary of the AI Act", *op. cit.*
[254] S. ARSÈNE, « Le système de crédit social en Chine : la discipline et la morale », *Réseaux*, 2021, p. 58.
[255] A. STROWEL, « L'intelligence artificielle : vers une régulation européenne par la gestion des risque », *Les pages : obligations, contrats et responsabilités*, 2021, p. 1.
[256] Commission européenne, « Communiqué de presse : Entrée en vigueur du règlement européen sur l'intelligence artificielle », *op. cit.*
[257] Commission européenne, « Communiqué de presse : Entrée en vigueur du règlement européen sur l'intelligence artificielle », *op. cit.*

biométriques à des données biométriques précédemment fournies »[258]. Son unique objectif est d'assurer qu'un individu est bien celui qu'il prétend être, de confirmer son identité dans le but d'avoir accès à un service, un local, de déverrouiller un dispositif[259]. Tandis que l'identification biométrique est « la reconnaissance automatisée de caractéristiques physiques, physiologiques, comportementales ou psychologiques humaines aux fins d'établir l'identité d'une personne physique en comparant ses données biométriques à des données biométriques de personnes stockées dans une base de données »[260].

La catégorisation biométrique est quant à elle « le classement de personnes physiques dans certaines catégories sur la base de leurs données biométriques »[261]. Ces catégories sont multiples et diverses, elles concernent notamment le sexe, l'âge, la couleur des yeux, …[262].

Les systèmes de reconnaissance des émotions permettent la reconnaissance ou la déduction des émotions ou des intentions de personnes physiques sur la base de leurs données biométriques[263].

Ces trois systèmes relèvent dans certaines situations des pratiques interdites visées par le chapitre 2 de l'AI Act[264], tandis que dans d'autres contextes particuliers et sous le respect de strictes conditions, leur utilisation est parfois autorisée[265]. Il convient de noter que, lorsqu'ils ne relèvent pas de l'interdiction énoncée à l'article 5 du règlement, ces systèmes sont considérés comme des systèmes à haut risque, en tant que systèmes autonomes mentionnés à l'annexe III du règlement[266].

b) Critère temporel

Au sein du concept d'identification biométrique à distance, des distinctions sont encore opérables. Initialement, les parlementaires de l'Union européenne souhaitaient que la reconnaissance faciale soit purement et simplement prohibée, le Comité européen de la protection des données et le Contrôleur européen de la protection des données partageaient cette volonté[267]. Cependant, il a été décidé qu'en fonction du contexte et des modalités, son niveau

[258] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024, précité, art. 3, 36).
[259] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024, précité, cons. 15.
[260] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024, précité, art. 3, 35).
[261] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024, précité, cons. 16 et art. 3, 40).
[262] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024, précité, cons. 16.
[263] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024, précité, art. 3, 40).
[264] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024, précité , art. 5, §1, f), g), h).
[265] B. DOCQUIR, *op. cit.*, p. 239.
[266] B. DOCQUIR, *op. cit.*, p. 260.
[267] F. COTON, *op. cit*,, p. 189.

de risque diffère et sa réglementation est corrélativement prévue soit par le chapitre 2 soit par le chapitre 3.

Il convient de distinguer les systèmes d'identification à distance « en temps réel » définis comme « un système d'identification biométrique à distance dans lequel l'acquisition des données biométriques, la comparaison et l'identification se déroulent sans décalage temporel important et qui comprend non seulement l'identification instantanée, mais aussi avec un léger décalage afin d'éviter tout contournement des règles »[268] ; de ceux « *a posteriori* » définis de façon résiduelle comme « un système d'identification biométrique à distance autre qu'un système d'identification biométrique à distance en temps réel »[269]. L'identification des personnes a lieu sur base d'un contenu préalablement collecté[270] et est dite retardée lorsqu'elle opère après un « délai significatif »[271]. Cependant, le Contrôleur européen de la protection des données et le Comité européen de la protection des données dénoncent le manque de définition de ce critère[272].

i. « *A posteriori* »

Les systèmes d'identification biométrique à distance « *a posteriori* » relèvent de la catégorie des systèmes à haut risque, ils ressortent des domaines listés à l'annexe III du règlement[273]. Ceux-ci doivent donc respecter les exigences générales contraignantes établies au chapitre 3 : une mise en place d'un système de gestion des risques[274], le respect des critères de qualité des données utilisées pour l'entrainement, la validation et les tests concernant la pertinence, la représentativité, l'exactitude et l'exhaustivité[275] afin de prévenir notamment les biais discriminatoires[276], la tenue de registres documentant le fonctionnement du système et les processus décisionnels[277], la transparence et l'information des utilisateurs[278], une supervision

[268] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024, précité, art. 3, 42).
[269] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024, précité, art. 3, 43).
[270] Commission européenne, « Intelligence artificielle – Questions et réponses », 1er août 2024, https://ec.europa.eu/commission/presscorner/detail/fr/qanda_21_1683 (date de dernière consultation : 30 mars 2025).
[271] P. KELLER, « La perte de la face : réglementation et contestation de la surveillance biométrique », *in Reconnaissance faciale : Défis techniques, juridiques et éthiques* (sous la dir. de M. BOZZO-REY, A. BRUNO-ERNST et C. WROBEL), Paris, Editions Panthéon-Assas, 2024, p. 88.
[272] P. KELLER, *op. cit.*, p. 88.
[273] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024, précité, annexe 3, 1) ; A. BENSOUSSAN, J. BENSOUSSAN et V. BENSOUSSAN-BRULÉ, *Le règlement européen sur l'intelligence artificielle*, Bruxelles, Bruylant, 2025, p. 75.
[274] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024, précité, art. 9.
[275] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024, précité, art. 10.
[276] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024, précité, art. 11 et annexe 4.
[277] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024, précité, art. 12.
[278] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024, précité, art. 13.

humaine du système afin d'assurer un contrôle humain effectif sur les décisions prises par le système[279], et, dernièrement, des exigences en matière de performance technique portant sur l'exactitude, la robustesse et la cybersécurité du système[280] [281].

Dans le domaine répressif, des formalités supplémentaires sont prévues. Lorsque le système est utilisé dans le cadre d'une enquête pénale visant à rechercher spécifiquement une personne soupçonnée ou condamnée pour une infraction, une autorisation préalable émanant d'une autorité judiciaire ou administrative compétente dont la décision est contraignante et susceptible d'appel, est requise[282].

Le considérant 95 appelle à la prudence et à la modération : « Les conditions d'identification biométrique à distance *a posteriori* ne devraient en aucun cas constituer une base permettant de contourner les conditions applicables en ce qui concerne l'interdiction et les exceptions strictes pour l'identification biométrique à distance en temps réel »[283].

ii. « En temps réel »

Concernant les dispositifs « à distance, en temps réel et dans des espaces accessibles au public », comme précité, le règlement prévoit une interdiction de principe, clé de la protection de la vie privée, caractéristique de la démocratie[284].

Cette distinction sur base du critère de temporalité pose question et laisse perplexe. En effet, il est difficile de conclure sur cet élément qu'une gradation quant aux impacts sur les droits fondamentaux et donc sur l'encadrement législatif puisse être établie[285]. Le seul fait que la reconnaissance soit effectuée « *a posteriori* » ne pallie pas les ingérences que celle-ci engendre[286]. Par ailleurs, le degré d'intrusion d'un traitement de données biométriques ne dépend pas exclusivement du fait qu'il implique ou non une identification en temps réel[287].

[279] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024, précité, art 14.
[280] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024, précité, art. 15.
[281] H.-W. MICKLITZ, « Règlement européen sur l'intelligence artificielle, normes harmonisées et effets externes », *Revue internationale de droit économique*, 2023, p. 75.
[282] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024, précité, art. 26, 10).
[283] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024, précité, cons. 95.
[284] A. BENSOUSSAN, J. BENSOUSSAN et V. BENSOUSSAN-BRULÉ, *op. cit.* , p. 71.
[285] Entretien avec Rémy Farge, formateur à la Ligue des droits humains, tenu le 24 mars 2025.
[286] Entretien avec Rémy Farge, formateur à la Ligue des droits humains, tenu le 24 mars 2025.
[287] P. KELLER, *op. cit.*, p. 88.

c) Interdiction relative

Cependant, la législation prévoit également trois exceptions en son article 5, premier alinéa, point h), permettant aux états membres de l'Union européenne d'autoriser l'usage de la reconnaissance faciale « en temps réel » dans des espaces accessibles au public à des fins répressives[288]. Les états sont libres de prévoir la possibilité d'autoriser totalement ou partiellement son utilisation dans les limites et les conditions énumérées au paragraphe premier, premier alinéa, point h), et aux paragraphes 2 et 3[289]. Auquel cas, ils devront prévoir dans leur droit national les modalités nécessaires à la demande, à la délivrance, à l'exercice des autorisations requises, de même qu'organiser le contrôle et l'établissement de rapports[290]. L'ensemble de ces règles doit être communiqué à la Commission dans les trente jours de leur adoption[291]. À l'inverse, les états membres, conformément au droit de l'Union, peuvent adopter des lois plus restrictives quant à l'utilisation des systèmes d'identification biométrique à distance[292].

En Belgique, un nouveau gouvernement fédéral se met en place et devra décider soit de prohiber de façon générale cette technologie soit d'opter pour un cadre plus souple en intégrant les exceptions proposées par le règlement dans sa législation. Le 31 janvier 2025, l'accord de gouvernement Arizona a été communiqué. Celui-ci semble prendre un tournant sécuritaire en ce qu'il renforce les services de police par une présence accrue dans certains lieux sensibles et par l'élargissement de leurs pouvoirs répressifs[293]. S'il continue dans ce raisonnement, nous pouvons craindre qu'un cadre juridique intégrant les exceptions soit adopté.

Ces exceptions sont les suivantes : « i) la recherche ciblée de victimes spécifiques d'enlèvement, de la traite ou de l'exploitation sexuelle d'êtres humains, ainsi que la recherche de personnes disparues ; ii) la prévention d'une menace spécifique, substantielle et imminente pour la vie ou la sécurité physique de personnes physiques ou d'une menace réelle et actuelle ou réelle et prévisible d'attaque terroriste ; iii) la localisation ou l'identification d'une personne

[288] Ligue des droits humains, « Reconnaissance faciale : 'La Belgique doit interdire totalement cette technologie de surveillance' », 31 janvier 2025, https://www.liguedh.be/reconnaissance-faciale-la-belgique-doit-interdire-totalement-cette-technologie-de-surveillance/ (date de dernière consultation : 30 mars 2025).
[289] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024, précité, art. 5, §5.
[290] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024, précité, art. 5, §5.
[291] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024, précité, art. 5, §5.
[292] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024, précité, art. 5, §5.
[293] Ligue des droits humains, « Accord 'Arizona' : recul préoccupant pour les droits sociaux et droits des étranger.ères et tournant sécuritaire confirmé », 2025, https://www.liguedh.be/accord-arizona-recul-preoccupant-pour-les-droits-sociaux-et-droits-des-etranger%c2%b7eres-et-tournant-securitaire-confirme/ (date de dernière consultation : 15 avril 2025).

soupçonnée d'avoir commis une infraction pénale, aux fins de mener une enquête pénale, d'engager des poursuites ou d'exécuter une sanction pénale pour des infractions visées à l'annexe II et punissables dans l'état membre concerné d'une peine ou d'une mesure de sûreté privatives de liberté d'une durée maximale d'au moins quatre ans »[294]. Il est à noter qu'est uniquement visée leur utilisation dans un contexte répressif [295]. En marge de ces interdictions, l'encadrement juridique de la reconnaissance faciale à des fins commerciales, telles que l'utilisation de systèmes visant à prévenir le vol à l'étalage dans les commerces, demeure à préciser[296]. Sous prétexte d'une nécessité pour l'économie numérique européenne, l'utilisation de ces systèmes à la maison, sur le lieu de travail, et dans d'autres endroits par le biais d'appareils personnels utilisant la reconnaissance faciale est envisageable[297].

En réalité, les limites de ces exceptions sont imprécises, ambigües et de nombreuses infractions pénales tombent dans le champ d'application de ces exceptions[298]. Au sein de l'annexe II du règlement, une liste des infractions pénales justifiant le recours à l'identification biométrique à distance en temps réel est dressée : terrorisme, viol, traitre des êtres humains, trafics de stupéfiants, d'armes, …[299]. Nous y retrouvons notamment la notion extrêmement large de « criminalité environnementale » qui recouvre tant le trafic d'espèces menacées que les incivilités et infractions liées aux dépôts clandestins[300]. Ainsi, sur la même base légale, un terroriste ou un individu abandonnant ses déchets dans un lieu non autorisé pourraient être sujets à cette technologie invasive. Une dérive quant à l'exception justifiée par la prévention d'un attentat est également à craindre au vu des définitions floues du terrorisme[301].

En conclusion, bien que le Parlement européen ait tenté d'instaurer une interdiction absolue de l'identification biométrique à distance notamment en introduisant des amendements prohibant les systèmes d'intelligence artificielle qui créent ou étendent les bases de données de reconnaissance faciale par extraction non ciblée d'images faciales sur Internet ou par vidéosurveillance[302], le règlement établit un cadre législatif relativement permissif car il crée

---

[294] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024, précité, art. 5, §1, h).
[295] B. BERTRAND, *op. cit.*, p. 83.
[296] P. KELLER, *op. cit.*, p. 83.
[297] P. KELLER, *op. cit.*, p. 87.
[298] Ligue des droits humains, « Reconnaissance faciale : 'La Belgique doit interdire totalement cette technologie de surveillance' », *op. cit.*
[299] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024, précité, annexe 2.
[300] Ligue des droits humains, « Reconnaissance faciale : 'La Belgique doit interdire totalement cette technologie de surveillance' », *op. cit.*
[301] Liga voor mensen rechten, « Waarom er nood is aan een Belgisch verbod op gezichtsherkenningstechnologie in de openbare ruimte », https://mensenrechten.be/pagina/nota-gezichtsherkenning (date de dernière consultation : 16 avril 2025).
[302] P. KELLER, *op. cit.*, p. 82.

de nombreuses dérogations qui d'autant plus, sont mal définies[303]. La légitimation, dans certaines circonstances, de formes de surveillance biométrique de masse initiée par l'intelligence artificielle engendre un risque d'abus et d'élargissement progressif de leur recours[304].

[303] C. BERTHÉLÉMY, « Mais que fait l'Europe ? », La *Chronique de la Ligue des droits humains asbl*, 2024, n° 208, pp. 17-19.
[304] C. BERTHÉLÉMY, *op. cit.*, pp. 17-19.

TITRE 3 : ANALYSE D'IMPACT DE LA RECONNAISSANCE FACIALE SUR LES DROITS FONDAMENTAUX

« Dire qu'on ne se soucie pas d'un droit parce qu'on ne l'utilise pas personnellement est la chose la plus antisociale que l'on puisse dire. Ce que cela signifie, c'est "Je me fiche des autres". En particulier lorsque cela est dit par quelqu'un qui occupe une position de privilège. Si vous êtes un homme riche, âgé et blanc au sommet de l'échelle sociale, vous n'avez pas à vous soucier des lois, à vous soucier du droit, car la société est organisée pour protéger vos intérêts. Ce sont toujours les minorités qui doivent faire face aux risques les plus élevés." E. SNOWDEN, extrait du documentaire « Nothing to hide », 2017[305].

Chapitre 1 : Atteinte aux droits fondamentaux

Section 1 : Notion

Les droits fondamentaux, autrefois appelés « droits de l'homme », partagent la particularité commune d'être protégés par des sources multiples nationales ou conventionnelles, écrites ou non, répétant, et par cela asseyant, la fondamentalité d'un droit[306]. Toute activité répressive doit préalablement observer le plein respect des droits fondamentaux, et cela peu importe la technologie dont il est fait usage[307]. Au niveau conventionnel et européen, nous retrouvons la Convention européenne des droits de l'homme et la Charte des droits fondamentaux de l'Union européenne, qui bénéficient toutes deux d'un statut privilégié en ce qu'une juridiction européenne attitrée interprète les droits qu'elles garantissent[308]. La Charte des droits fondamentaux s'impose aux institutions et organes de l'Union européenne. Il en découle que lorsque du droit dérivé est créé, celui-ci doit respecter la Charte[309]. Elle s'impose également aux états membres lorsqu'ils mettent en œuvre le droit de l'Union[310]. Les états membres doivent donc s'y conformer lorsqu'ils appliquent le règlement européen sur

[305] E. DE BUISSERET HARDY, « La reconnaissance faciale en procès ! », *La Chronique de la Ligue des droits humains* asbl, 2024, n° 208, p. 3.
[306] G. ROSOUX, « Panorama de la protection juridictionnelle nationale des droits fondamentaux : qui est le juge des droits fondamentaux en Belgique ? », *in Contentieux des droits fondamentaux* (sous la dir. de F. KRENC, F. BOUHON et C. DEPREZ), Limal, Anthemis, 2021, p. 9.
[307] F.R.A., « Technologie de reconnaissance faciale : considérations relatives aux droits fondamentaux dans le contexte de l'application de la loi », *op. cit.*, p. 22.
[308] G. ROSOUX, *op. cit.*, p. 9.
[309] P. GILLIAUX, « La force obligatoire de la Charte des droits fondamentaux de l'Union européenne », *Rev. trim. D. H.*, 2020, p. 78.
[310] P. GAÏA, « La Charte des droits fondamentaux de l'Union européenne », *Revue française de droit constitutionnel*, 2004, p. 238.

l'intelligence artificielle. L'article 27 de ce règlement impose en ce sens qu'une analyse d'impact des systèmes d'intelligence artificielle à haut risque sur les droits fondamentaux soit réalisée par les déployeurs[311]. Cette analyse devrait également être réalisée lorsque nous nous trouvons dans une situation qui autorise l'utilisation de systèmes d'identification biométrique à distance, en temps réel, dans les lieux accessibles au public[312].

Certains droits de l'Homme sont considérés comme des droits de *ius cogens*, cela implique que nous ne pouvons jamais y déroger[313]. Cependant, tous les droits fondamentaux ne présentent pas un caractère parfaitement absolu et en fonction des circonstances, il peut y être porté atteinte[314]. Cela apparait notamment dans les articles 8 à 11 de la Convention européenne des droits de l'Homme[315]. Nous retrouvons dans le deuxième paragraphe de ces articles une clause de limitation qui établit une méthode afin d'évaluer les atteintes aux droits, à travers un triple test. L'ingérence doit être prévue par la loi, reposée sur une base légale, doit poursuivre un but légitime énuméré dans la clause et enfin être nécessaire dans une société démocratique, c'est-à-dire être proportionnée au but poursuivi et répondre à besoin social impérieux[316]. La Charte des droits fondamentaux, en son article 52, §1, exige également que ces restrictions soient prévues par la loi, nécessaires et « répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui »[317].

À la lecture de l'AI Act, nous comprenons que nous ne sommes pas à l'abri d'être confrontés à la reconnaissance faciale. Dans ce chapitre, nous exposons un échantillon des droits pouvant être mis à mal par son utilisation et de quelle façon. Les droits fondamentaux concernés dépendent fortement de l'objectif, du contexte et de l'ampleur de l'utilisation de cette technologie[318]. Mais, dans tous les cas, elle a une implication sur un large éventail de droits fondamentaux[319]. L'Agence des droits fondamentaux de l'Union européenne déplore que les quelques analyses d'impact ne se penchent que sur des questions techniques et délaissent le sujet des droits fondamentaux, par un manque de connaissance sur la manière dont l'intelligence

[311] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024, précité, art. 27.
[312] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024, précité, art. 5, §2, al. 2 et cons. 34.
[313] P. MAKABA, « L'incorportaion de la convention européenne des droits de l'homme dans l'ordre juridique britannique », *Rev. trim. dr. h.*, 2000, p. 19.
[314] P. MAKABA, *op. cit.*, p. 19.
[315] C.E.D.H., art. 8-11.
[316] C.E.D.H. art 8-11, §2
[317] Charte des droits fondamentaux de l'Union européenne, *J.O.U.E.*, 26 octobre 2012, C326, art. 52.
[318] M. O'FLAHERTY, « Facial recognition technology and fundamental rights", *E.D.P.L.*, 2020, p. 171.
[319] F.R.A., « Bien préparer l'avenir : l'intelligence artificielle et les droits fondamentaux », *Office des publications de l'Union européenne*, 2021, p. 5, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2021-artificial-intelligence-summary_fr.pdf (date de dernière consultation : 18 mars 2025).

artificielle affecte ces droits[320]. Le problème est chronologique. D'abord, d'importants investissements sont réalisés dans les équipements de vidéosurveillance. Ensuite, l'installation et les tests ont lieu. Enfin, tardivement, à la suite de ces actions et en raison d'une interpellation d'un organe de contrôle ou de l'opinion public, la question de leur impact sur la population et sur les droits fondamentaux est abordée[321].

L'ensemble des droits fondamentaux repose sur la dignité fondamentale de la personne, consacrée au premier article de la Charte des droits fondamentaux, droit inviolable[322]. Le contrôleur européen de la protection des données a relevé que les éléments inhérents de la reconnaissance faciale que sont la marchandisation et l'objectivation des visages des individus, par le biais d'algorithmes, au profit d'entreprises privées ou de la surveillance étatique à grande échelle, portent atteinte à la dignité[323]. Les individus sont perçus comme des objets, leur visage étant considéré comme une simple plaque d'immatriculation[324]. « L'impact que les technologies perçues comme des outils de surveillance peuvent avoir sur la vie des individus est en mesure d'être si important qu'il en vient à affecter leur capacité à mener une vie dans la dignité »[325].

Section 2 : Atteinte à la liberté d'expression, de réunion et d'association

Pour qu'un état puisse se proclamer démocratique, celui-ci doit considérer la liberté d'expression et d'information comme en étant la pierre angulaire[326]. Ce droit est inscrit à l'article 11, §1 de la Charte des droits fondamentaux et à l'article 10 de la CEDH[327]. Un autre

[320] F.R.A., « Bien préparer l'avenir : l'intelligence artificielle et les droits fondamentaux », *Office des publications de l'Union européenne*, *op. cit.*, p. 6.
[321] A. WAVREILLE, « Reconnaissance faciale : fuyez, vous êtes filmé.es … et identifié.es », *La Chronique de la Ligue des droits humains asbl*, 2023, n° 203, p. 5.
[322] Charte des droits fondamentaux de l'Union européenne, *J.O.U.E.*, 26 octobre 2012, C326, art. 1 ; E.D.R.I., « Ban Biometric Mass Surveillance : A set of fundamental rights demands for the European Commission and EU Member States », Bruxelles, 2020, p. 21, https://edri.org/wp-content/uploads/2020/05/Paper-Ban-Biometric-Mass-Surveillance.pdf (date de dernière consultation : 25 mars 2025).
[323] E.D.R.I., *op. cit.*, p. 23.
[324] E.D.P.B., « Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement », 26 avril 2023, p. 15, https://www.edpb.europa.eu/system/files/2023-05/edpb_guidelines_202304_frtlawenforcement_v2_en.pdf (date de dernière consultation : 9 mai 2025).
[325] E.D.R.I., *op. cit.*, p. 22.
[326] F.R.A., « Technologie de reconnaissance faciale : considérations relatives aux droits fondamentaux dans le contexte de l'application de la loi », *op. cit.*, p. 33.
[327] Charte des droits fondamentaux de l'Union européenne, *J.O.U.E.*, 26 octobre 2012, C326, art. 11, §1 ; C.E.D.H., art. 10 ; F.R.A., « Technologie de reconnaissance faciale : considérations relatives aux droits fondamentaux dans le contexte de l'application de la loi », *op. cit.*, p. 33.

droit est fortement lié à la liberté d'expression : la liberté de réunion et d'association. Ce droit est garanti par l'article 12 de la Charte des droits fondamentaux, par l'article 11 de la CEDH.[328].

La reconnaissance faciale porte atteinte à ces droits fondamentaux en ce qu'elle entraine la perte essentielle d'une de ses conditions qui est l'anonymat de groupe. Ce droit primordial dans une société libre offre une certaine protection aux individus afin qu'ils puissent s'exprimer et s'associer librement, sans crainte de représailles[329]. Les tribunaux allemands ont d'ailleurs confirmé ce raisonnement en jugeant illégale la publication sur les réseaux sociaux de photos prises lors d'une manifestation, relevant l'effet néfaste sur la liberté d'association[330]. Au Royaume-Uni, la Cour d'appel a également donné raison au plaignant dans l'affaire Ed Bridges v. South Wales Police, s'indignant de l'utilisation de camions de police banalisés équipés de caméras de reconnaissance faciale lors d'une manifestation pacifique[331].

Pour ces raisons, les politiques concernant la vidéosurveillance devraient d'autant plus être prudentes et respectueuses de l'anonymat lorsque les dispositifs sont placés sur des terrains reflétant les idées politiques, religieuses ou sociales comme les églises, les cliniques pratiquant l'avortement, les lieux de manifestation, etc[332]. A Cologne, les autorités ont installé un système de reconnaissance faciale dans les environs de bars LGBTQIA+, de lieux de cultes, de cabinets médicaux ou d'avocats[333]. Chloé Berthélémy, conseillère chez EDRi, alerte sur la non-nécessité pour les autorités de récolter ce genre d'informations et accuse les systèmes de reconnaissance faciale de pousser naturellement vers ces dérives[334].

Récemment, nous retrouvons une illustration de cette problématique en Hongrie où le gouvernement du Premier ministre Viktor Orbán a pris une énième mesure restreignant les droits de la communauté LGBTQ+[335]. En mars 2025, une loi ayant pour objectif d'interdire la

---

[328] Charte des droits fondamentaux de l'Union européenne, *J.O.U.E.*, 26 octobre 2012, C326, art. 12 ; C.E.D.H., art. 11.
[329] F.R.A., « Technologie de reconnaissance faciale : considérations relatives aux droits fondamentaux dans le contexte de l'application de la loi », *op. cit.*, p. 33.
[330] F.R.A., « Technologie de reconnaissance faciale : considérations relatives aux droits fondamentaux dans le contexte de l'application de la loi », *op. cit.*, p. 33.
[331] M. BOZZO-REY, A. BRUNO-ERNST et C. WROBEL, « Introduction », *in Reconnaissance faciale : Défis techniques, juridiques et éthiques* (sous la dir. de M. BOZZO-REY, A. BRUNO-ERNST et C. WROBEL), Paris, Editions Panthéon-Assas, 2024, p. 12.
[332] NLets, « Privacy impact assessment report for the utilization of recognition technologies to identify subjects in the field », 2011, p. 19, https://www.eff.org/files/2013/11/07/09_-_facial_recognition_pia_report_final_v2_2.pdf (date de dernière consultation : 25 mars 2025).
[333] A. WAVREILLE, *op. cit.*, p. 5.
[334] A. WAVREILLE, *op. cit.*, p. 5.
[335] X. « Hongrie : des milliers de manifestants protestent à Budapest contre une loi interdisant la Gay Pride », RTBF, 2025, https://www.rtbf.be/article/hongrie-des-milliers-de-manifestants-protestent-a-budapest-contre-une-loi-interdisant-la-gay-pride-11526924 (date de dernière consultation : 15 mars 2025).

Marche des fiertés, également connue sous le nom de « Gay Pride », a été adoptée par les députés hongrois[336]. Peter Drenth, rapporteur permanent adjoint sur les droits humains du Congrès des pouvoirs locaux et régionaux du Conseil de l'Europe, s'inquiète de cette nouvelle législation et déplore que cette dernière autorise les autorités à recourir aux technologies de reconnaissance faciale afin d'identifier les individus en infraction et de les condamner à une amende[337].

Il est notamment reproché à ces dispositifs de dissuader les citoyens à participer à des manifestations. Se sachant surveillés ceux-ci sont incités à modifier leur comportement, à exprimer différemment leurs opinions ou à tout simplement ne plus le faire ; les individus s'autocensurent[338]. Ce phénomène est appelé le « Chilling effect »[339]. La résistance aux institutions, notamment par des mouvements de désobéissance, pourtant cruciaux dans l'acquisition d'avancées sociales, morales et politiques, se verrait alors presque impossible[340].

Ce constat est inquiétant étant donné que le droit de réunion pacifique « permet aux personnes de contribuer collectivement à modeler la société dans laquelle elles vivent d'une manière puissante mais pacifique et protège la capacité de chacun à exercer son autonomie tout en étant solidaire d'autrui »[341].

Comme susmentionné, le terrorisme est une des infractions pénales listées à l'annexe du II du règlement européen sur l'intelligence artificielle qui justifie l'usage de l'identification biométrique à distance en temps réel. Dès lors, des organisations de protestations pacifiques pourraient se voir criminalisées et considérées comme des organisations terroristes dans le but de justifier leur soumission à cette technologie[342]. En novembre 2024, le Vlaams Belang souhaitait que les groupes « Black Lives Matter » et « Extinction Rebellion » soient inscrits sur

---

[336] M. P., « La Hongrie de Viktor Orban interdit la marche des fiertés et va utiliser la reconnaissance faciale pour cibler les participants », Le Parisien, 2025, https://www.leparisien.fr/societe/la-hongrie-de-viktor-orban-interdit-la-marche-des-fiertes-et-va-utiliser-la-reconnaissance-faciale-pour-cibler-les-participants-19-03-2025-WNQ72DER4JETZKJWA2MUJVLWTU.php (date de dernière consultation : 15 mars 2025).

[337] Conseil de l'Europe, « Le rapporteur du Congrès est profondément préoccupé par l'amendement constitutionnel en Hongrie », 16 avril 2025, https://www.coe.int/fr/web/portal/-/-we-should-all-be-proud-of-pride-congress-rapporteur-deeply-concerned-by-constitutional-amendment-in-hungary (dernière consultation : 5 mai 2025).

[338] Amnesty International France, « J.O. 2024 : Pourquoi la vidéosurveillance algorithmique pose problème », 2024, https://www.amnesty.fr/liberte-d-expression/actualites/pourquoi-la-videosurveillance-algorithmique-pose-probleme-cameras-technologies (dernière consultation : 28 mars 2025).

[339] A. WAVREILLE, *op. cit.*, p. 5.

[340] J. MARGNYS, « La vie privée, pour quoi faire ? Exigence démocratique et reconnaissance faciale », *La Chronique de la Ligue des droits humains asbl*, 2024, n° 208, p. 10.

[341] F.R.A., « Technologie de reconnaissance faciale : considérations relatives aux droits fondamentaux dans le contexte de l'application de la loi », *op. cit,* p. 33.

[342] Liga voor mensen rechten, *op. cit.*

la liste belge des organisations terroristes, ceux-ci pourraient alors être sujets à la reconnaissance faciale[343].

Section 3 : Atteinte à la vie privée

a) Données personnelles

La problématique des bases de données est indissociable de l'avènement des systèmes d'identification et de surveillance de masse[344]. Lorsqu'une technologie de reconnaissance faciale est utilisée, celle-ci implique des étapes comme l'enregistrement initial des images, leur conservation, ainsi que leur comparaison avec des bases de données dans le but d'opérer une identification, une correspondance[345]. Cette procédure constitue une atteinte à deux droits intrinsèquement liés : le droit à la protection des données personnelles, consacré à l'article 8 de la Charte et le droit au respect de la vie privée, consacré à l'article 7 de la Charte, à l'article 8 de la Convention européenne des droits de l'homme, ainsi qu'à l'article 22 de la Constitution belge[346]. Comme mentionné précédemment, les données biométriques sont dites « sensibles », elles sont relatives à l'intimité de la vie privée des personnes[347]. De plus, elles ont la particularité d'être non révocables, elles viennent directement du corps et ne peuvent être modifiées. Elles méritent donc une protection maximale afin de garantir la vie privée des individus[348]. Certains imaginent les données comme un cinquième pouvoir, à côté des quatre autres : législatif, exécutif, judiciaire et médiatique[349].

En 2008, la Cour européenne des droits de l'homme, éveillée quant aux dangers de la biométrie, a rendu une décision engageante sur la problématique de la conservation des données biométriques[350]. *In casu*, dans l'affaire Marper c. Royaume-Uni, il s'agissait plus particulièrement de l'enregistrement d'empreintes digitales et de données génétiques mais il nous parait pertinent et transposable à la technologie de reconnaissance faciale. La Cour

---

[343] Liga voor mensen rechten, *op. cit.*
[344] S. PREUSS-LAUSSINOTTE, « Bases de données personnelles et politiques de sécurité : une protection illusoire ? », *Cultures & Conflits*, 2006, p. 1.
[345] T. MADIEGA et H. MILDEBRATH, « Réglementation de la reconnaissance faciale au sein de l'Union européenne », *Service de recherche du Parlement européen*, 2021, p. 18, https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_FR.pdf (date de dernière consultation : 28 mars 2025).
[346] Charte des droits fondamentaux de l'Union européenne, *J.O.U.E.*, 26 octobre 2012, C326, art. 7 et 8 ; C.E.D.H., art. 8 ; Const. art. 22 ; T. MADIEGA et H. MILDEBRATH, *op. cit.*, p. 18.
[347] C.N.I.L., « Reconnaissance faciale : pour un débat à la hauteur des enjeux », *op. cit.*, p. 6.
[348] C.N.I.L., « Reconnaissance faciale : pour un débat à la hauteur des enjeux », *op. cit.*, p. 6.
[349] P. LHOUTELLIER, « Données, technologies et systèmes d'information de sécurité : le contexte européen dans le temps de la présidence française de l'Union européenne », *Cahiers de la sécurité et de la justice*, 2022, p. 156.
[350] Cour. eur. dr. h., arrêt Marper c. Royaume-Uni du 4 décembre 2008 ; F. CROUZATIER-DURAND, *Fiches de libertés publiques et droits fondamentaux*, Paris, Ellipses, 2021, p. 81.

réaffirme que le fait de mémoriser des données relatives à la vie privée d'un individu viole l'article 8 de la CEDH[351]. Elle ajoute que la vie privée est une notion qui doit être largement interprétée, recouvrant autant l'intégrité physique que morale de la personne et englobant de nombreux pans de son identité physique et sociale[352]. En ce sens, la Ligue des droits humains appelle à concevoir la vie privée comme un bien devant être préservé et non comme une contrainte devant être levée[353].

L'utilisation de la reconnaissance faciale requiert la création ou l'accroissement de bases de données, justifiée, à tort, par un objectif de protection des personnes[354]. En effet, des erreurs et des dérives peuvent être observées : des risques de saisie incorrecte, d'homonymie ainsi que des détournements d'usage (les données recueillies pour une finalité sont utilisées pour une autre non prévue)[355]. Il convient alors de se demander quelles garanties sont mises en place afin de préserver la vie privée des individus.

Les articles 12 à 22 du RGPD reconnaissent aux personnes concernées une série de droits lorsqu'un traitement de leurs données personnelles est effectué dans un cadre non répressif[356].Les personnes dont les données sont recueillies par la police ou la justice à des fins répressives ont des droits consacrés par la loi du 30 juillet 2018 : le droit à l'information, le droit d'accès, le droit à la rectification ou à l'effacement[357] .

Cependant, ces droits, censés pallier à cette intrusion dans la vie privée des individus, ne sont que difficilement exerçables[358]. Même lorsqu'ils sont expressément prévus, la protection des individus est de plus en plus formelle[359]. Les problèmes liés à la récolte des données sont fréquents malgré de rares plaintes[360]. La cause de ce constat est une complexité

[351] F. CROUZATIER-DURAND, *op. cit.*, p. 81.
[352] F. CROUZATIER-DURAND, *op. cit.*, p. 81.
[353] J. MARGNYS, *op. cit.*, p. 10.
[354] S. PREUSS-LAUSSINOTTE, « Bases de données personnelles et politiques de sécurité : une protection illusoire ? », *op. cit.*, p. 6.
[355] S. PREUSS-LAUSSINOTTE, « Bases de données personnelles et politiques de sécurité : une protection illusoire ? », *op. cit.*, p. 10.
[356] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, précité, art. 12-22.
[357] Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, art. 36-39, *M.B.*, 5 septembre 2018, p. 68616 ; C. FORGET, *op. cit.*, p. 16.
[358] C. FORGET, *op. cit.*, p. 22.
[359] S. PREUSS-LAUSSINOTTE, « Bases de données personnelles et politiques de sécurité : une protection illusoire ? », *op. cit.*, p. 6.
[360] F.R.A., « Under watchful eyes : biometrics, EU IT systems and fundamental rights », *Office des publications de l'Union européenne*, 2018, p. 17, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-biometrics-fundamental-rights-eu_en.pdf (date de dernière consultation le 1er avril 2025).

des procédures couplée à un manque de sensibilisation et de compréhension quant à la manière d'exercer leurs droits[361].

b) Migration

Une catégorie de la population mondiale voit sa vie privée d'autant plus bafouée quand il est question de migration. Les droits des étrangers sont souvent précaires, voire inexistants, celui à la vie privée ne fait pas exception[362]. Les politiques migratoires poursuivent la même finalité de catégorisation et de suivi de plus en plus rigoureux[363]. Pour atteindre cet objectif, de nouvelles politiques de sécurité sont adoptées afin de recueillir les données des étrangers, les échanger, établir des connexions et ainsi les contrôler davantage[364].

Les étrangers sont souvent perçus à l'écart de la collectivité nationale et en conséquence on leur attribue un statut différent et bien souvent plus contraignant que les nationaux[365]. L'instauration de dispositions répressives à leur égard influence leur réputation et entraine les nationaux à les considérer comme des délinquants en puissance profondément dangereux[366].

L'effet dissuasif pouvant mener à un risque d'exclusion, observé quant à la liberté de réunion et d'expression, s'observe également dans le domaine de la migration[367]. En effet, la Rapporteuse spéciale de l'ONU sur les formes contemporaines de racisme a mis en lumière l'impact de l'usage des technologies biométriques sur l'accès aux services de base essentiels comme les soins de santé[368]. Certains migrants se privent d'une prise en charge médicale pour éviter d'être identifiés comme « sans papier »[369].

Eurodac est un fichier européen qui reprend les données dactyloscopiques, les empreintes digitales, des migrants postulant à la politique européenne d'asile, collectées par les états membres[370]. Initialement, cette base de données a été créée afin d'appliquer la convention

---

361 F.R.A., « Under watchful eyes : biometrics, EU IT systems and fundamental rights », *op. cit.*, p. 17.
362 J.-F. FOEGLE, « La déconstruction de la vie privée des demandeurs d'asile », *Mémoires*, 2017, p. 14.
363 J.-F. FOEGLE, *op. cit.*., p. 12.
364 J.-F. FOEGLE, *op. Cit.*., p. 12.
365 D. LOCHAK, « L'image de l'étranger au prisme des lois sur l'immigration » *in Figures de l'étranger, quelles représentations pour quelles politique ?*, Paris, Gisti, 2013, p. 36.
366 D. LOCHAK, *op. cit.*., p. 37.
367 Défenseur des droits, « Technologies biométriques : l'impératif respect des droits fondamentaux », 2021, p. 14, https://www.defenseurdesdroits.fr/rapport-technologies-biometriques-limperatif-respect-des-droits-fondamentaux-274 (date de dernière consultation : 1er avril 2025).
368 Défenseur des droits, *op. cit.*, p. 14.
369 Défenseur des droits, *op. cit.*, p. 14.
370 L. ROUSVOAL, « L'accès des services répressifs aux données de migrants et réfugiés présentes dans le fichier Eurodac » *in Les données numériques des migrants et des réfugiés sous l'angle du droit européen* (sous la dir. de S. TURGIS), Rennes, Presses universitaires de Rennes, 2020, p. 82.

de Dublin, afin de gérer le flux migratoire et prévenir toute fraude[371]. La justification de ce fichage est d'offrir la possibilité aux états de s'assurer qu'un étranger se trouvant illégalement sur son territoire n'a pas effectué une demande d'asile dans un autre état membre[372]. Par la suite, l'accès au fichier a été élargi aux autorités répressives dans une finalité de lutte contre certaines infractions comme le terrorisme[373]. Un phénomène a alors été observé. Certains demandeurs d'asile, désemparés, en sont réduits à brûler leurs doigts afin de brouiller leurs empreintes et de pouvoir soumettre à nouveau une demande de régularisation[374]. Afin de neutraliser ce procédé, au relevé des empreintes digitales se sont ajoutées les images faciales des demandeurs d'asiles[375]. Sur pied du règlement européen 2024/1358, les états membres doivent collecter les données biométriques, y compris les images faciales, des demandeurs de protection internationale âgés d'au moins 6 ans[376]. Cet élargissement de la base de données constitue davantage une intrusion dans la vie privée de ces personnes.

Un autre système basé sur la reconnaissance faciale a été mis à l'essai en 2018, en Grèce, en Hongrie et en Lettonie pour renforcer la forteresse de l'Union européenne[377]. Ce dispositif, appelé *iBorderCtrl*, soumet les personnes exilées voulant traverser une frontière à un interrogatoire virtuel qui fonctionne par détecteur de mensonges[378]. L'algorithme analyse chaque détail des expressions via la reconnaissance faciale et conclut à la véracité ou l'inauthenticité de leurs propos[379]. Des relations entre les expressions faciales, les états affectifs, le mensonge et le risque sont erronément établies au départ d'une chaine d'hypothèses qui n'est

[371] L. ROUSVOAL, *op. cit.*., p. 82.
[372] S. PREUSS-LAUSSINOTTE, « L'élargissement problématique de l'accès aux bases de données européennes en matière de sécurité », *Cultures & Conflits*, 2009, p. 83.
[373] L. ROUSVOAL, *op. cit.*., p. 82.
[374] Règlement (UE) 2024/1358 du Parlement européen et du conseil du 14 mai 2024 relatif à la création d'Eurodac » pour la comparaison des données biométriques aux fins de l'application efficace des règlements (UE) 2024/1351 et (UE) 2024/1350 du Parlement européen et du Conseil et de la directive 2001/55/CE du Conseil et aux fins de l'identification des ressortissants de pays tiers et apatrides en séjour irrégulier, et relatif aux demandes de comparaison avec les données d'Eurodac présentées par les autorités répressives des États membres et par Europol à des fins répressives, modifiant les règlements (UE) 2018/1240 et (UE) 2019/818 du Parlement européen et du Conseil et abrogeant le règlement (UE) n o 603/2013 du Parlement européen et du Conseil, cons. 19, *J.O.U.E.*, 22 mai 2024, série L ; E. DE BUISSERET HARDY, *op. cit.*, p. 4.
[375] E. DE BUISSERET HARDY, *op. cit.*, p. 5.
[376] Règlement (UE) 2024/1358 du Parlement européen et du conseil du 14 mai 2024, précité, art. 15-17.
[377] Amnesty International France, « Les technologies automatisées et l'avenir de la forteresse Europe », 2019, https://www.amnesty.org/fr/latest/news/2019/03/automated-technologies-and-the-future-of-fortress-europe/ (date de dernière consultation le 9 avril 2025).
[378] Amnesty International France, « Cinq outils numériques utilisés aux frontières contre les personnes exilées », 2024, https://www.amnesty.fr/refugies-et-migrants/actualites/technologies-et-reconnaissance-faciale-aux-frontieres-la-derive-contre-les-personnes-exilees (date de dernière consultation : 9 avril 2025).
[379] Amnesty International France, « Cinq outils numériques utilisés aux frontières contre les personnes exilées », *op. cit.*

pas validée scientifiquement[380]. Le sort de ces personnes est à nouveau mis aux mains d'un système déshumanisé et fondé sur l'intelligence artificielle par nature biaisée[381].

Section 4 : Outil de discrimination

La reconnaissance faciale impacte également le droit à la non-discrimination. Nous retrouvons ce principe de non-discrimination à l'article 2 du T.U.E., à l'article 10 du T.F.U.E., aux articles 20 et 21 de la Charte, mais aussi dans des dispositions particulières et plus précises de plusieurs directives de l'Union européenne[382]. Ces prescrits obligent l'Union européenne à lutter contre toute discrimination fondée sur un certain nombre de motifs et à garantir l'égalité en droit[383]. Parmi ces motifs, nous retrouvons notamment la race, les origines ethniques ou sociales, la religion, le sexe, …[384].

Afin que la reconnaissance faciale puisse s'effectuer, le recours à des logiciels algorithmiques est indispensable. Il convient de s'attarder sur le fonctionnement de ceux-ci.

Le fonctionnement de l'intelligence artificielle, basé sur la reproduction, contribue à l'aggravation et à la rapidité de la progression des inégalités dans nos sociétés[385]. La technologie algorithmique se nourrit des données que nous lui fournissons lors de son entrainement. Si ces données sont biaisées, ses décisions le seront aussi[386].

Le Parlement européen, a lui-même fait état des études empiriques indiquant que la plupart des systèmes de reconnaissance faciale présentent encore des performances techniques relativement limitées et que les logiciels de détection faciale peuvent engendrer deux types d'erreur[387]. Un faux négatif arrive lorsque le logiciel n'est pas capable d'identifier un visage présent sur une image[388]. Un faux positif, beaucoup plus préjudiciable pour la personne

---

[380] R. FARGE, « Reconnaissance automatique des émotions, une valeur probante à haut risque », *La Chronique de la Ligue des droits humains* asbl, 2024, n° 208, p. 23.
[381] Amnesty International France, « Les technologies automatisées et l'avenir de la forteresse Europe », *op. cit.*
[382] T.U.E., art. 2 ; T.F.U.E., art.10 ; Charte des droits fondamentaux de l'Union européenne, *J.O.U.E.*, 26 octobre 2012, C326, art. 20-21 ; F.R.A., « Bien préparer l'avenir : l'intelligence artificielle et les droits fondamentaux », *op. cit.*, p. 10.
[383] F.R.A., « Bien préparer l'avenir : l'intelligence artificielle et les droits fondamentaux », *op. cit.*, p. 10.
[384] Charte des droits fondamentaux de l'Union européenne, *J.O.U.E.*, 26 octobre 2012, C326, art. 21.
[385] M. LEVY, *Sortez vos données du frigo, une entreprise performante avec la Data et l'IA*, Paris, Dunod, 2021, p. 147.
[386] M. LEVY, *op. cit.*, p. 147.
[387] F. DECHAMPS et M. ADAM, « IA et reconnaissance faciale – Un outil prisé…mais à quel prix ? Analyse du cas Clearview AI », *D.P.O. News,* 2023, p. 21.
[388] F. DECHAMPS et M. ADAM, *op. cit.*, p. 21.

concernée, se produit lorsque le programme reconnait erronément un visage, lui attribue une mauvaise identité[389].

Joy Adowaa Buolamwini, chercheuse et militante, a réalisé une expérience afin de mettre en lumière les biais dont peuvent être affectés les algorithmes[390]. Mille visages ont été soumis à un logiciel de reconnaissance faciale et le constat est sans appel : les personnes ayant la peau foncée, et si de surcroît ce sont des femmes, ont été plus difficilement identifiées[391]. Une étude du MIT a également mis en lumière l'iniquité des individus face à la reconnaissance faciale : les hommes blancs étant le mieux identifiés, et les femmes noires l'étant le moins bien[392]. Les tests réalisés à Zaventem par la police fédérale de l'aéroport, entre 2017 et 2019, ont eux aussi relevé la fiabilité douteuse de cette technologie. En effet, de nombreux faux positifs ont été décelés à cause de la couleur de peau, du port de lunettes ou de la présence de barbe et/ou moustache, des individus[393]. En France, lors de l'expérimentation de la vidéosurveillance algorithmique pendant les jeux olympiques, des personnes sans-abris ont été considérées comme des colis abandonnés[394].

Les conséquences de ces identifications erronées peuvent être dramatiques : des individus parfaitement innocents se retrouvent derrière les barreaux. Aux Etats-Unis, lorsque la police a recours à ces logiciels, dix fois plus d'identifications sont fausses lorsqu'il s'agit de reconnaitre une personne noire ou asiatique plutôt qu'une personne blanche[395]. Le Washington Post a écrit un article dénonçant qu'au moins huit Américains avaient été arrêtés à tort ; les enquêteurs faisant une confiance aveugle à la technologie de reconnaissance faciale et négligeant alors des étapes de l'enquête[396]. Ils utilisent cette technologie comme un raccourci pour identifier et arrêter des suspects sans autre élément de preuve[397].

La reconnaissance faciale est également une menace à la non-discrimination en raison d'une simplification et d'une augmentation du profilage racial exercé par la police envers les

---

[389] F. DECHAMPS et M. ADAM, *op. cit.*, p. 21.
[390] L. SALMONA, *Politiser les cyberviolences – Une lecture intersectionnelle des inégalités de genre sur internet*, Paris, Le Cavalier Bleu, 2023, p. 30.
[391] L. SALMONA, *op. cit..*, p. 30.
[392] M. LEVY, *op. cit*, p. 147.
[393] Organe de contrôle de l'information policière, « Rapport intermédiaire », *op. cit.*, p. 4.
[394] Amnesty International France, « Voici comment le gouvernement a prolongé la vidéosurveillance algorithmique », *op. cit.*
[395] L. SALMONA, *op. cit.*, p. 30.
[396] D. MACMILLAN, D. OVALLE et A. SCHAFFER, « Arrested by AI : Police ignore standards after facial regonition matches », The Washington Post, 2025, https://www.washingtonpost.com/business/interactive/2025/police-artificial-intelligence-facial-recognition/ (date de dernière consultation : 6 avril 2025).
[397] D. MACMILLAN, D. OVALLE et A. SCHAFFER, *op. cit.*

non-blancs lors des contrôles et des enquêtes[398]. Celle-ci disposerait ainsi d'un outil capable de directement cibler certaines catégories de la population. Une étude indique que les personnes dans la tranche d'âge de 10 à 20 ans et de couleur de peau sombre sont sur-surveillés, elles sont ciblées par les dispositifs et par la suite interpellées[399]. Certains poussent cette critique jusqu'à soutenir que la reconnaissance faciale serait « un des moyens par lesquels le suprémacisme blanc d'antan serait parvenu, malgré les apparences, à se perpétuer »[400].

Chapitre 2 : Politique de surveillance

Section 1 : Notion

La reconnaissance faciale, et donc l'identification, est mise au profit de la surveillance. Dans ce chapitre, nous approfondissons cette notion ainsi que ses enjeux. Initialement, l'identification et la surveillance étaient perçues comme deux activités séparées[401]. La surveillance, qui se limitait jusqu'à aujourd'hui au suivi de la trace d'un individu, prend aujourd'hui une nouvelle dimension[402].

En effet, grâce aux différents et nouveaux processus d'identification, il est d'autant plus facile d'identifier et donc de surveiller un individu. Pour ce faire, les nouvelles technologies d'identification et de surveillance utilisent les caractéristiques innées et inchangeables des particuliers, appelées le « bios »[403].

La surveillance est un terme relativement courant. Il nous parait cependant opportun de la définir. La surveillance est « l'acquisition, temporaire, permanente, ou à durée variable d'information »[404]. Ces informations concernent des objets sociaux, c'est-à-dire, les individus et leurs interactions[405]. La collecte de ces informations poursuit nécessairement un objectif, ce dernier est généralement « l'intervention ou l'obtention d'un bénéfice extérieur à la connaissance pure »[406].

---

398 V. AUBERT, « Reconnaissance faciale et racisme : clarifier les enjeux du débat », *Raison-publique*, 2024, p. 3.
399 S. CALLENS, *Démocratie et télésurveillance*, Villeneuve d'Ascq, Presses universitaires du Septentrion, 2002, p. 24.
400 V. AUBERT, *op. cit.*. , p. 3
401 A. CEYHAN, « Editorial. Identifier et surveiller : les technologies de sécurité », *Cultures & Conflits*, 2006, pp. 7-9.
402 A. CEYHAN, « Editorial. Identifier et surveiller : les technologies de sécurité », *op. cit.*, pp. 7-9.
403 A. CEYHAN, « Editorial. Identifier et surveiller : les technologies de sécurité », *op. cit.*, pp. 7-9.
404 S. LEMAN-LANGLOIS, *Sphères de surveillance*, Montréal, Les Presses de l'Université de Montréal, 2011, p. 10.
405 S. LEMAN-LANGLOIS, *op. cit.*., p. 10.
406 S. LEMAN-LANGLOIS, *op. cit.*., p. 11.

Vient alors la question du « par qui » et du « pourquoi » sommes-nous surveillés ? La surveillance est inhérente au genre humain et depuis que la technologie existe, est liée étroitement à cette dernière[407].

L'objectif de la surveillance des individus n'est pas simplement d'assouvir une curiosité malsaine mais bien de parvenir à une gestion efficace des corps des individus en dépit d'une hétérogénéité sociale[408]. L'identification comme instrument de surveillance permet au gouvernement d'augmenter son pouvoir de contrôle sur les comportements des individus[409]. Le contexte de crise anti-terroriste, renforcé depuis les attentats du World Trade Center à New-York en 2001, constitue un terrain propice à la prolifération de la surveillance et amène une logique anticipatoire : il n'est plus question de contrer un évènement en comprenant sa cause mais plutôt de réorganiser l'ordre social pour prévenir un évènement peu probable mais théoriquement possible[410].

La décision de généraliser cet outil de contrôle est particulièrement politique[411]. Par cette prise de position, l'élu prouve, de façon concrète et matérielle, son action sur les problèmes de sa localité[412]. Le politicien justifie son recours à la vidéosurveillance en vantant cette dernière comme un instrument essentiel dans la lutte contre la délinquance et le terrorisme[413]. Il promet une meilleure sécurité à la population grâce au triple effet de la vidéosurveillance[414]. Dans un premier temps, cette dernière dissuade, ensuite elle permet de repérer des faits et finalement d'identifier leurs auteurs[415].

Section 2 : Efficacité

Nous avons précédemment exposé les faiblesses techniques des systèmes de reconnaissance faciale lors du processus d'identification. Dans cette section, nous nous

---

[407] R. BELLANOVA, P. DE HERT et S. Gutwirth, « Variations sur le thème de la banalisation de la surveillance », *Mouvements*, 2010, p. 47.
[408] V. MARISCAL, « Compte-rendu de : Olivier Aïm, Les théories de la surveillance. Du panoptique aux Surveillances Studies », *La Nouvelle Revue du Travail,* 2021, p. 1.
[409] NLets, *op. cit.*, p. 19,
[410] F. TRÉGUER, *Technopolice : La surveillance policière à l'ère de l'intelligence artificielle*, Quimperlé, Editions Divergences, 2024, p. 84.
[411] L. MUCCHIELLI, « La vidéosurveillance réduit-elle la criminalité ? » *in L'enseignement universitaire en milieu carcéral : Expériences comparées entre la France et l'Italie* (sous la dir. de P. PACINI VOLPE), Nîmes, Champ social, 2021, p. 256.
[412] E. HEILMANN, « La vidéosurveillance, un mirage technologique et politique », *op. cit.*, p. 123.
[413] L. MUCCHIELLI, « La vidéosurveillance réduit-elle la criminalité ? », *op. cit.*„ p. 257.
[414] L. MUCCHIELLI, « La vidéosurveillance réduit-elle la criminalité ? », *op. cit.*„ p. 257.
[415] L. MUCCHIELLI, « La vidéosurveillance réduit-elle la criminalité ? », *op. cit.*„ p. 257.

interrogeons de façon plus générale sur l'efficacité de la surveillance dans la lutte contre la criminalité.

A propos de la surveillance, Michel Foucault a théorisé et interprété la notion du Panoptique de Jeremy Bentham dans son ouvrage « Surveiller et Punir »[416]. À l'origine, « panoptique » est un principe de base de la conception architecturale carcérale basée sur la visibilité continue[417]. Cette architecture instaure une possibilité permanente d'être surveillé sans moyen de savoir si nous le sommes vraiment[418]. L'auteur explique qu'une possibilité de surveillance omniprésente augmente certes le pouvoir des autorités et l'obligation des citoyens à obéir mais mène surtout à une intériorisation du regard de leurs surveillants, ceux-ci adopteront alors inconsciemment le comportement attendu[419]. Ce dispositif permet à la surveillance « d'être continue dans ses effets même si elle est discontinue dans son action et cela maintient l'individu disciplinaire dans son assujettissement »[420].

C'est dans cette logique d'accroissement de la surveillance des individus que se sont mis en place et se sont créés différents dispositifs, de la simple caméra à la caméra capable d'effectuer une reconnaissance faciale. La biométrie étend alors le dispositif panoptique à l'ensemble de la société[421].

Pourtant vendue comme une ou voire la solution miracle aux maux de la société, la vidéosurveillance algorithmique n'aurait en réalité pas l'effet promis sur la délinquance[422]. En l'absence de preuve formelle de l'efficacité de la technologie, justifier son utilisation en termes de nécessité et de proportionnalité se révèle complexe[423].

Il est à noter que le nombre d'étude confirmant ou infirmant l'efficacité de l'utilisation de la vidéosurveillance afin de réduire la criminalité ne prolifère pas.

La multiplication de caméras ne limiterait pas la délinquance mais ne ferait que la déplacer sur un autre territoire[424]. De plus, leur soi-disant effet dissuasif serait presque

---

[416] B.-E. HARCOURT, *La société d'exposition*, Paris, Le Seuil, 2020, p. 77.
[417] A. LECLERCQ-VANDELANNOITTE, H. ISAAC et M. KALIKA, *Travail à distance et e-management : organisation et contrôle en entreprise*, Paris, Dunod, 2013, p. 45.
[418] A. LECLERCQ-VANDELANNOITTE, H. ISAAC et M. KALIKA, *op. cit.*, p. 45.
[419] B.-E. HARCOURT, *op. cit.*, p. 77.
[420] A. LECLERCQ-VANDELANNOITTE, H. ISAAC et M. KALIKA, *op. cit.*, p. 45.
[421] A.-L. FORTIN-TOURNÈS, « La reconnaissance faciale : une remise en question des champs de l'éthique et du politique ? », *in Reconnaissance faciale : Défis techniques, juridiques et éthiques* (sous la dir. de M. BOZZO-REY, A. BRUNO-ERNST et C. WROBEL), Paris, Editions Panthéon-Assas, 2024, p. 181.
[422] T. GOFF, « Le faux et coûteux miracle de la vidéosurveillance », *Après-demain,* 2010, pp. 28-30.
[423] B. PEETERS, *op. cit.*, p. 160.
[424] N. BOURGOIN, *La révolution sécuritaire (1976-2012)*, Nîmes, Champ Social Editions, 2013, p. 165.

inexistant[425]. Ces dispositifs auraient exclusivement une utilité concernant les vols de véhicules ou dans les véhicules dans des parkings surveillés par des caméras, en revanche les délits violents ou les vols ne seraient eux que rarement contrés[426].

Pour que la vidéosurveillance soit efficace, *a fortiori* celle algorithmique et permettant l'identification biométrique, les habitants doivent participer à la construction du projet afin d'attribuer à l'objet technique une destination sociale et éviter son rejet[427]. Sinon, la mise en place d'un tel dispositif constitue alors une perte d'argent et la rentabilité d'une telle action ne serait, comme susmentionnée, qu'électorale. Le criminologue Jelle Janssens, de l'université de Gand, s'inquiète de cette instrumentalisation des caméras par les politiques[428].

Section 3 : Capitalisation de la surveillance

La prolifération des caméras de surveillance algorithmiques n'est malheureusement pas motivée uniquement par la poursuite de l'intérêt général[429]. Un réel marché, business lucratif, s'est déployé et influence négativement l'action publique[430]. En 2016, plus de 500 entreprises mettant au point des technologies de surveillance vendaient leurs produits à des états[431]. Le taux de croissance de ce marché est à deux chiffres, a atteint les 16 milliards de dollars en 2014 et n'a pas été impacté par la crise[432]. Cela s'explique par une forte sollicitation, un cadre juridique clément et un regard approbateur des pouvoirs publics[433]. Tout cela se développe dans un contexte de capitalisation de la surveillance dans lequel nos données sont continuellement récoltées et cédées au plus offrant[434].

Les élus se fient à des personnes qui s'attribuent le titre d'expert et à des consultants fortement implantés sur le marché de la sécurité[435]. Le terme employé est celui de « marché de la sécurité » et non de « marché de la surveillance ». Le marché de la sécurité ne cesse de

[425] Q. NOIRFALISSE, *op. cit.*
[426] Q. NOIRFALISSE, *op. cit.*
[427] E. HEILMANN, « La vidéosurveillance, une réponse efficace à la criminalité ? », *Criminologie*, 2003, p. 101.
[428] Q. NOIRFALISSE, *op. cit.*
[429] E. HEILMANN, « La vidéosurveillance, un mirage technologique et politique », *op. cit.*, p. 123.
[430] E. HEILMANN, « La vidéosurveillance, un mirage technologique et politique », *op. cit*, p. 123.
[431] Assemblée générale des Nations Unies « Conseil des droits de l'homme : Surveillance et droits de l'homme : Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression », 2021, https://documents.un.org/doc/undoc/gen/g19/148/77/pdf/g1914877.pdf (date de dernière consultation : 5 avril 2025).
[432] L. MUCCHIELLI, « A quoi sert la vidéosurveillance de l'espace public ? : Le cas français d'une petite ville 'exemplaire' », *Déviance et société*, 2016, p. 45.
[433] L. MUCCHIELLI, « A quoi sert la vidéosurveillance de l'espace public ? : Le cas français d'une petite ville 'exemplaire' », *op. cit.*, p. 45.
[434] A.- L. FORTIN-TOURNÈS, *op. cit.*, p. 181.
[435] E. HEILMANN, « La vidéosurveillance, un mirage technologique et politique », *op. cit.*, p. 123.

s'accroitre et, à l'inverse de celui de la surveillance, n'est pas réglementé[436]. Il est à observer que le terme « sécurité », bien qu'il ne soit pas un synonyme, remplace alors à tort celui de « surveillance »[437]. Cet amalgame permet une meilleure acceptation par le citoyen d'atteinte à ses droits, sous couvert d'un besoin de sécurité[438].

Les entreprises se servent du facteur « peur » qui légitime la surveillance, afin de vendre de nouveaux équipements aux gouvernements[439]. Ces entreprises vont notamment se servir de l'argument du « droit à la sécurité ». Elles s'attèlent à convaincre les citoyens que leur demande de sécurité peut être satisfaite au travers des innovations technologiques[440].

C'est au nom de ce soi-disant « droit à la sécurité » que des mesures restrictives de liberté, via notamment les technologies de reconnaissance faciale, sont justifiées[441]. Thomas Hobbes relève effectivement l'importance de la sécurité dans le contrat social : la sécurité des individus est assurée en échange de l'abandon de leurs libertés[442]. Cependant, il est important de noter qu'aucune convention européenne ou internationale n'établit explicitement un droit à la sécurité des personnes et des biens[443].

De plus, une dangereuse confusion s'opère entre le droit à la sécurité et le droit à la sûreté au détriment de ce dernier[444]. L'article 3 de la Déclaration universelle des droits de l'homme de 1948 dispose que « Tout individu a droit à la vie, à la liberté et à la sûreté de sa personne »[445]. Le droit à la sûreté est le droit à la protection de la liberté individuelle[446]. Il tend à préserver le citoyen de tout privation de liberté arbitraire ou injustifiée réalisée par une autorité publique[447]. Nous ne pouvons pas en déduire une obligation des états à instaurer des mesures pour éviter aux individus d'être confrontés à des actes criminels[448]. Ces deux notions sont donc

---

[436] S. LEMAN-LANGLOIS, *op. cit.*, p. 19.
[437] S. LEMAN-LANGLOIS, *op. cit.*, p. 19.
[438] S. LEMAN-LANGLOIS, *op. cit.*, p. 19.
[439] Z. BAUMAN, D. BIGO, P. ESTEVES, E. GUILD, V. JABRI, D. LYON et R.B.J. WALKER, « Repenser l'impact de la surveillance après l'affaire Snowden : sécurité nationale, droits de l'homme, démocratie, subjectivité et obéissance », *Culture & Conflits*, 2015, p. 164.
[440] P. LHOUTELLIER, *op. cit.*, p. 156.
[441] S. PREUSS-LAUSSINOTTE, « Bases de données personnelles et politiques de sécurité : une protection illusoire ? », *op. cit.*, p. 3.
[442] S. PREUSS-LAUSSINOTTE, « Bases de données personnelles et politiques de sécurité : une protection illusoire ? », *op. cit.*, p. 3.
[443] C. LAZERGES, « Le droit à la sécurité a-t-il effacé le droit à la sûreté ? L'exemple de la loi 'Sécurité globale' », *La Revue des droits de l'homme*, 2021, p. 2.
[444] C. LAZERGES, *op. cit.*, p. 2.
[445] Déclaration universelle des droits de l'homme, signée à Paris le 10 décembre 1948, art. 3.
[446] C. LAZERGES, *op. cit.*, p. 2.
[447] C. DE TERWAGNE, *op. cit.*, p. 9.
[448] C. DE TERWAGNE, *op. cit.*, p. 9.

antinomiques en ce que l'une tend à protéger les droits des individus et que l'autre justifie leurs restrictions[449].

Section 4 : Risque de glissement

Une autre raison nous pousse à vouloir nous protéger contre ces technologies biométriques : le contexte politique. Une innovation technologique dans un pays considéré comme « libre » pourrait être utilisée à des fins répressives dans un pays ne garantissant pas les mêmes droits et libertés[450]. Les laboratoires occidentaux développant ces innovations prennent le risque d'alimenter un projet de société contraire à leurs valeurs[451]. Il est primordial de se demander ce qu'il adviendrait de ces technologies, installées et acceptées dans un régime démocratique, si celui-ci se transforme en régime autoritaire.

Il est certain que le pouvoir discrétionnaire de certains services s'amplifierait[452]. Ces dispositifs répressifs augmentent l'asymétrie de pouvoir entre gouvernants et gouvernés, caractéristique d'un système anti-démocratique[453].

Nous pouvons notamment avoir un aperçu de cet usage par un régime autoritaire voire totalitaire dans lequel la société est constamment surveillée : la Chine[454]. Depuis 2014, le pays a mis en place un large programme de contrôle de sa population notamment via des logiciels de reconnaissance faciale[455]. Outre le problématique « social scoring » susmentionné, la technologie biométrique participe à l'identification et à la répression des Ouïghours[456]. Elle est omniprésente dans la région autonome ouïghoure du Xinjiang où près d'un million de membres de ce groupe ethnique est arbitrairement retenu captif dans des camps dits de rééducation[457].

La reconnaissance faciale est également utilisée dangereusement lors de conflits. Amnesty International a publié un rapport dénonçant l'usage de cette technologie aux fins de fragmentation, de ségrégation et de contrôle de la population palestinienne dans les territoires

---

[449] S. PREUSS-LAUSSINOTTE, « Bases de données personnelles et politiques de sécurité : une protection illusoire ? », *op. cit.*, p. 3.
[450] J.-Y. HEURTEBISE, « Innovation, histoire et géopolitique en « Chine » : Revanche technologique, mimétisme impérialiste et techno-autoritarisme », *Monde chinois*, 2020, p. 94.
[451] J.-Y. HEURTEBISE, *op. cit.*, p. 94.
[452] R. FARGE, *op. cit.*, p. 23.
[453] J. MARGNYS, *op. cit.*, p. 10.
[454] D. REYHAN, « Génocide Ouïghour : cheminement d'un projet colonial », *Monde chinois*, 2021, p. 19.
[455] P. DAMBLY et A. BEELEN, *(R)évolution de l'intelligence artificielle : vers un cadre juridique et technique de l'IA*, Limal, Anthémis, 2023, p. 381.
[456] J.-Y. HEURTEBISE, *op. cit.*, p. 94.
[457] Amnesty International France, « Des entreprises de l'UE vendent des outils de surveillance à des responsables d'atteintes aux droits humains en Chine », 2020, https://www.amnesty.org/fr/latest/press-release/2020/09/eu-surveillance-sales-china-human-rights-abusers/ (date de dernière consultation : 11 avril 2025).

palestiniens occupés, restreignant leur liberté de déplacement[458]. Ce nouveau système de reconnaissance faciale instauré par le gouvernement israélien se nomme « Red Wolf » et se retrouve notamment aux checkpoints d'Hébron, territoire palestinien occupé, afin de déterminer si un individu est habilité à entrer dans une zone[459]. De nombreux Palestiniens et Palestiniennes n'ont d'autre choix que de passer par ce point de contrôle pour accéder à la quasi-totalité des biens et services essentiels, exercer une activité professionnelle ou poursuivre leurs études, maintenir une vie familiale ou encore recevoir des soins de santé[460].

Chapitre 3 : Stratégie de lutte

Section 1 : Sensibilisation

Dans ces conditions, la question de l'acceptabilité de la biométrie par les citoyens se pose. Cette notion ne doit pas être confondue avec l'acception[461]. L'acceptabilité désigne l'action d'accepter avec résignation, sans révolte, ne résultant pas d'un libre choix mais influencée par d'autres facteurs[462]. Il ressort qu'une grande majorité de la population n'est pas directement réfractaire à l'augmentation de la surveillance. Plusieurs facteurs expliquent cela : la familiarité, la peur et l'amusement, les loisirs[463]. Afin de contrer ces facteurs, une sensibilisation des citoyens est nécessaire.

a) Information

La sensibilisation commence par l'information. Au sein du premier titre de ce travail, nous déplorions un manque de transparence quant à la disposition géographique des caméras de vidéosurveillance. Lorsqu'un système de vidéosurveillance est installé, la Commission de la protection de la vie privée doit en être notifiée au plus tard la veille du jour de sa mise en service[464]. Cependant, il ressort d'une étude de 2016, que ce registre est incomplet et que même

[458] Amnesty International, « Apartheid automatisé : Comment la reconnaissance faciale fragmente, ségrègue et contrôle les Palestiniens et les Palestiniennes dans les TPO », 2023, p. 7, https://www.amnesty.org/fr/documents/mde15/6701/2023/fr/ (date de dernière consultation : 17 avril 2025).
[459] Amnesty International, « Apartheid automatisé : Comment la reconnaissance faciale fragmente, ségrègue et contrôle les Palestiniens et les Palestiniennes dans les TPO », *op. cit.*, p. 77.
[460] Amnesty International, « Apartheid automatisé : Comment la reconnaissance faciale fragmente, ségrègue et contrôle les Palestiniens et les Palestiniennes dans les TPO », *op. cit.*, p. 49.
[461] A. CEYHAN, « 'Acceptabilité' de la biométrie : linéaments d'un cadre analytique », *in L'identification biométrique : Champs, acteurs, enjeux et controverses* (sous la dir. de A. CEYHAN et P. PIAZZA), Paris, Editions de la maison des sciences de l'homme, 2011, p. 396.
[462] A. CEYHAN, « 'Acceptabilité' de la biométrie : linéaments d'un cadre analytique », *op. cit.*, p. 396.
[463] Z. BAUMAN, D. BIGO, P. ESTEVES, E. GUILD, V. JABRI, D. LYON et R.B.J. WALKER, *op. cit.*, p. 164.
[464] Loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance, précitée, art. 5-7.

les autorités publiques ne respectent cette obligation[465]. En effet, le double de caméras inscrites au registre a été recensé[466].

En France, la même problématique a été mise en lumière par l'association « La Quadrature du Net ». Cette dernière combat la censure, la surveillance et œuvre à la protection des libertés fondamentales dans l'environnement numérique[467]. Cette association a mis sur pied le projet « Technopolice », qui s'est aussi déployé en Belgique[468]. Ce collectif identifie et localise les dispositifs de surveillance à Bruxelles et fournit une carte régulièrement mise à jour qui répertorie notamment l'emplacement des caméras publiques et privées dans l'espace public bruxellois[469].

b) Consentement

Une autre façon de sensibiliser le public passe par l'assurance de leur réel consentement à être soumis à ces technologies. Les systèmes fondés sur l'intelligence artificielle sont par nature complexes et pour certains opaques[470]. Il est naïf de présumer que les individus possèdent un niveau de connaissance suffisant pour comprendre le fonctionnement de ces systèmes ainsi que leurs impacts sur leur autonomie, sur leurs droits fondamentaux[471].

De plus, par sa nature « à distance », le système d'identification biométrique identifie des personnes physiques sans leur participation active[472]. Cette notion de participation n'est pas clairement définie dans l'AI Act mais elle semble être à l'antipode d'un consentement explicite[473].

Il serait alors opportun que des agents, à l'instar des tentatives du Métropolitan Police Service, expliquent le rôle de la technologie, que des prospectus soient distribués et que des panneaux d'information soient installés[474]. Cependant, afin d'obtenir un consentement

[465] P. DE KEERSMAECKER et C. DEBAILLEUL, *op. cit.*, p. 3.
[466] P. DE KEERSMAECKER et C. DEBAILLEUL, *op. cit.*, p. 3.
[467] La Quadrature du Net, « Nous », https://www.laquadrature.net/nous/ (date de dernière consultation : 26 mars 2025).
[468] Carte interactive disponible sur : https://technopolice.be/
[469] N. BOCQUET, *op. cit.*, p. 10.
[470] 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.
[471] C. FONTES et C. PERRONE, *op. cit.*, p. 6.
[472] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024, précité, cons. 17 ; P. VOIGT et N. HULLEN, *The EU AI Act : Answers to frequently asked questions*, Berlin, Springer, 2024, p. 45.
[473] P. VOIGT et N. HULLEN, *op. cit.*, p. 45.
[474] C. FONTES et C. PERRONE, *op. cit.*, p. 6.

réellement éclairé, une condition de temps est nécessaire pour que les individus puissent y réfléchir posément et librement[475].

c) Mouvements citoyens

Des associations, dont la Ligue des droits humains, s'attèlent à alerter l'opinion public à travers différentes actions. La sensibilisation de la population vise à mettre en lumière les différents enjeux éthiques ainsi que les atteintes potentielles à leurs droits, afin que les citoyens en prennent pleinement conscience, soient correctement informés et puissent se positionner en connaissance de cause. Ces organisations ne se contentent pas d'informer mais agissent aussi concrètement en entreprenant des démarches juridiques. Celles-ci ont notamment réalisé une coalition nommée « Protect my face » et ont déposé une pétition au Parlement bruxellois afin de demander l'interdiction de la reconnaissance faciale dans l'espace public à Bruxelles[476].

Cette campagne au niveau national fait écho à une campagne à l'échelle européenne, « Reclaim Your Face », menée par l'ONG « EDRi » (European Digital Rights). Cette opération, portée par 110 organisations à travers 25 états membres, appelle à la fin de la surveillance biométrique de masse dans l'Union européenne[477]. EDRi réalise également un guide juridique et pratique évolutif afin de lutter contre ces technologies, via une approche fondée sur les droits humains[478].

Section 2 : Moyen institutionnel

La lecture de l'AI Act nous apprend que celui-ci interdit en principe l'identification biométrique à distance en temps réel, à des fins répressives, dans des espaces accessibles au public[479]. Cependant, les états membres peuvent, au moyen d'une loi nationale, permettre son utilisation dans certaines situations[480].

En 2024, le Festival des libertés, en partenariat avec la Ligue des droits humains, a organisé un procès fictif ainsi qu'un débat sur le sujet. En effet, dans l'hypothèse où l'Etat belge

[475] C. FONTES et C. PERRONE, *op. cit.*, p. 6.
[476] Ligue des droits humains, « Protectmyface », https://www.liguedh.be/une-petition-pour-interdire-la-reconnaissance-faciale-dans-lespace-public-bruxellois-2/ (date de dernière consultation : 9 avril 2025).
[477] E.D.R.I., « EDRi and Reclaim Your Face campaign recognised as Europe AI Policy leaders », 2024, https://edri.org/our-work/edri-reclaim-your-face-campaign-awarded/ (date de dernière consultation : 10 avril 2025).
[478] E.D.R.I., « How to fight Biometric Mass Surveillance after the AI Act : a legal and practical guide », 2024, https://edri.org/our-work/how-to-fight-biometric-mass-surveillance-after-the-ai-act-a-legal-and-practical-guide/ (date de dernière consultation : 11 avril 2025).
[479] Commission européenne, « Intelligence artificielle – Questions et réponses », *op. cit.*
[480] Commission européenne, « Intelligence artificielle – Questions et réponses », *op. cit.*

légifère et adopte une loi en ce sens, introduire un recours en annulation à la Cour constitutionnelle constituerait une stratégie de lutte. En vertu de l'article 1er de la loi spéciale sur la Cour constitutionnelle, cette dernière contrôle la conformité des lois à la lumière notamment des droits fondamentaux[481]. Si la Cour estime l'existence avérée de la violation de droits fondamentaux, la loi se verrait alors annulée.

Ce recours pourrait être introduit par l'A.S.B.L. Ligue des droits humains, en tant que personne morale justifiant d'un intérêt[482]. Cette dernière introduit des recours en justice lorsqu'elle estime qu'une disposition législative menace ou enfreint les libertés fondamentales[483].

[481] Loi spéciale du 6 janvier 1989 sur la Cour constitutionnelle, art. 1er, *M.B.*, 7 janvier 1989, p. 315 ; H. BORTELS, D. KEYARTS, W. VERRIJDT et L. DE GEYTER, « Loi spéciale sur la Cour constitutionnelle : De la compétence de la Cour constitutionnelle », *in Focus sur le droit de la procédure devant la Cour constitutionnelle et le Conseil d'Etat*, Malines, Wolters Kluwer, 2024, pp. 15-16.
[482] Loi spéciale du 6 janvier 1989 sur la Cour constitutionnelle, art. 2, al. 1er, 2°, *M.B.*, 7 janvier 1989, p. 315
[483] Ligue des droits humains, « Actions en justice », https://www.liguedh.be/en-action/actions-en-justice/ (date de dernière consultation : 8 mai 2025).

CONCLUSION

Ce mémoire s'inscrit dans un contexte particulièrement brûlant et contemporain, tant sur le plan juridique que sur le plan sociétal. La reconnaissance faciale n'est plus une invention futuriste mais est une technologie intégrée dans notre sphère privée, pour déverrouiller notre téléphone par exemple, mais aussi dans nos espaces publics à travers des expérimentations et des projets pilotes.

Au sein du premier titre, nous avons retracé l'évolution de la vidéosurveillance et abordé la notion complexe de biométrie. Nous faisons face à une réalité : les barrières techniques de la reconnaissance faciale ont disparu. Tout est matériellement mis en place pour accueillir et généraliser la reconnaissance faciale, qui est d'ailleurs souvent utilisée sans base légale, avec des expérimentations et des projets pilotes. Le simple fait qu'une innovation technologique existe implique-t-il que l'on doive nécessairement l'adopter sans discernement au nom du « progrès » ? Le recours à cette technologie n'est alors plus qu'un choix politique et éthique.

Le deuxième titre de ce mémoire est consacré à l'analyse de l'encadrement législatif de l'intelligence artificielle. Nous en avons appris davantage sur le sort réservé à la technologie de reconnaissance faciale par le règlement sur l'intelligence artificielle adopté récemment par l'Union européenne.

Il en ressort que différents régimes s'appliquent à la reconnaissance faciale en fonction notamment de la temporalité de son utilisation. Ce critère nous a laissés quelque peu perplexes compte tenu de l'impact que cette dernière peut avoir sur les droits fondamentaux, indépendamment du moment de son usage. De plus, même lorsque le régime proclame une interdiction stricte, celle-ci se révèle facultative. En effet, le règlement prévoit la possibilité pour les états d'assouplir l'interdiction de l'identification biométrique à distance en temps réel dans les espaces accessibles au public à des fins répressives via une loi nationale. À cet égard, la position du gouvernement belge suscite des inquiétudes légitimes compte tenu des signaux politiques actuels. Il convient de souligner que cette législation européenne exprime des préoccupations et instaure néanmoins certaines obligations et garanties afin de limiter les atteintes. Nous constatons et regrettons cependant un manque de clarté et de définition qui pourrait engendrer une généralisation et une banalisation des dispositions censées être exceptionnelles.

Ces réserves quant à l'identification biométrique trouvent leur fondement et leur justification dans la dernière partie de ce travail. Nos recherches ont confirmé que cette technologie était non seulement régulièrement défaillante, mais pouvait et portait déjà atteinte aux droits fondamentaux des individus comme la liberté d'expression, d'association et de réunion, la vie privée, ou l'interdiction de la discrimination. Une avancée sur le plan technologique peut, paradoxalement, entraîner un recul en matière de droits fondamentaux.

Cet affaiblissement des libertés est un terrain propice au développement de la surveillance de masse. Nous en sommes alors venus à nous questionner de façon plus générale sur les notions de surveillance et de sécurité. En effet, ces technologies sont présentées comme des instruments de sécurité et d'efficacité dans la lutte contre la criminalité. Cependant, leur impact réel demeure contestable et leur déploiement s'inscrit généralement dans une logique de rentabilité commerciale ou de contrôle politique. De plus, nous observons une capitalisation de la surveillance, une confusion entre sécurité et sûreté, ainsi qu'un risque de dérive autoritaire.

Une grande partie de la société reste peu sensibilisée à ces enjeux. Bien que la reconnaissance faciale présente des avantages et puisse s'avérer utile dans certains contextes, ses dérives potentielles ne doivent pas être sous-estimées. C'est pourquoi des associations, comme la Ligue des droits humains, s'attèlent à effectuer de la prévention et à entreprendre des actions afin de préserver nos libertés et droits fondamentaux. Il convient de ne pas céder à l'utopie ni de se complaire dans une position privilégiée propre aux systèmes démocratiques. Il est au contraire nécessaire d'adopter une vigilance lucide en considérant les risques de dérives qui se sont déjà matérialisés chez nous et ailleurs dans le monde.

BIBLIOGRAPHIE

Législation

Supranationale

- CEDH., art. 8-11.
- T.U.E., art. 2.
- T.F.U.E., art. 10, 16, 26, 114 et 288.
- Charte des droits fondamentaux de l'Union européenne, *J.O.U.E.*, 26 octobre 2012, C326, art. 1, 7, 8, 11, 12, 20, 21, 52.
- Déclaration universelle des droits de l'homme, signée à Paris le 10 décembre 1948, art. 3.
- Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection 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, art. 1-3 et 10, *J.O.U.E.*, 4 mai 2016, L 119, pp. 89-131.
- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, art. 2, 4, 9 et 12-22, *J.O.U.E.*, 4 mai 2016, L 119, pp. 1-88
- Règlement (UE) 2024/1358 du Parlement européen et du conseil du 14 mai 2024 relatif à la création d'Eurodac pour la comparaison des données biométriques aux fins de l'application efficace des règlements (UE) 2024/1351 et (UE) 2024/1350 du Parlement européen et du Conseil et de la directive 2001/55/CE du Conseil et aux fins de l'identification des ressortissants de pays tiers et apatrides en séjour irrégulier, et relatif aux demandes de comparaison avec les données d'Eurodac présentées par les autorités répressives des États membres et par Europol à des fins répressives, modifiant les règlements (UE) 2018/1240 et (UE) 2019/818 du Parlement européen et du Conseil et abrogeant le règlement (UE) n° 603/2013 du Parlement européen et du Conseil, cons. 19 et art. 15-17, *J.O.U.E.*, 22 mai 2024, série L.
- Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024, établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 202/1828, cons. 1, 3, 5, 14-17, 20 et 34, art. 3-5, 9-16, 26, 27, 50 et 113, annexe 2, 3 et 4, *J.O.U.E.*, 12 juillet 2024, série L.

- 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) 206 final, 21 avril 2021.

Nationale

- Const., art. 22.
- Loi spéciale du 6 janvier 1989 sur la Cour constitutionnelle, art. 1, 2, *M.B.*, 7 janvier 1989, p. 315.
- Loi du 5 août 1992 sur la fonction de police, art. 25/2,3 ; 44/2 ; 46/1,4,7,9,11 , *M.B.*, 22 décembre 1992, p. 27124.
- Loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance, art. 2, 3 et 5-8, *M.B.*, 31 mai 2007, p. 29529.
- 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, p. 33691.
- Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, art. 36-39, *M.B.*, 5 septembre 2018, p. 68616.
- A.R. du 18 décembre 2002 déterminant les infractions dont la constatation fondée sur des preuves matérielles fournies par des appareils fonctionnant automatiquement en l'absence d'un agent qualifié, fait foi jusqu'à preuve du contraire, art. 1er, *M.B.*, 25 décembre 2002, p. 58181.
- 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, Exposés introductifs, *Doc. parl.*, Ch. repr., sess. ord. 2017-2018, n° 54 2855/003, p. 12
- Proposition de loi modifiant l'arrêté royal du 18 décembre 2002 déterminant les infractions dont la constatation fondée sur des preuves matérielles fournies par des appareils fonctionnant automatiquement en l'absence d'un agent qualifié, fait foi jusqu'à preuve du contraire en ce qui concerne l'usage du téléphone portable au volant, *Doc. parl.*, Ch. repr., sess. ord. 2020-2021, n°55-1722/001.

- 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. parl.*, Ch. repr., sess. ord. 2019-2020, n° 55-1349/001, p. 11.

Française

- Loi n° 2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions, art. 10.

Jurisprudence

Supranationale

- C.J.U.E. (troisième ch.), *Vandemoortele c. Commission*, C-172/89, ECLI :UE :C :1990 :457.
- C.J.U.E. (gde ch.), S*chrems c. Data Protection Commissioner*, C-362/14, ECLI:EU:C:2015:650.
- C.J.U.E. (gde ch.), *Tele2 Sverige AB c. Post-och telestyrelsen*, C-203/15, ECLI:EU:C:2016:970.
- C.J.U.E. (gde ch.), *Privacy International c. Secretary of State for Foreign and Commonwealth Affairs e.a.*, C-623/17, ECLI:EU:2020:790.
- Cour. eur. dr. h., arrêt Marper c. Royaume-Uni du 4 décembre 2008
- Cour eur. dr. h., arrêt Big Brother Watch c. Royaume-Uni du 25 mai 2021.
- Cour eur. dr. h., arrêt Glukhin c. Russie du 4 juillet 2023.

Internationale

- Appelate Court, R v. the Chief Constable of South Wales Police, 11 août 2020, C1:2019/2670.

Doctrine

- ABOUT I. et DENIS V., *Histoire de l'identification des personnes*, Paris, La Découverte, 2010, pp. 3-4.
- ARSÈNE S., « Le système de crédit social en Chine : la discipline et la morale », *Réseaux*, 2021, p. 58.
- AUBERT V., « Reconnaissance faciale et racisme : clarifier les enjeux du débat », *Raison-publique*, 2024, p. 3.

- BAUMAN Z., BIGO D., ESTEVES P., GUILD E., JABRI V., LYON D. et WALKER R.B.J., « Repenser l'impact de la surveillance après l'affaire Snowden : sécurité nationale, droits de l'homme, démocratie, subjectivité et obéissance », *Culture & Conflits*, 2015, p. 164.
- BEELEN A., « RGPD et intelligence artificielle : ce qu'il faut savoir du nouveau règlement européen », *D.P.O. News*, 2025, pp. 12-13.
- BELLANOVA R., DE HERT P. et Gutwirth S., « Variations sur le thème de la banalisation de la surveillance », *Mouvements*, 2010, p. 47.
- BENSOUSSAN A., BENSOUSSAN J. et BENSOUSSAN-BRULÉ V., *Le règlement européen sur l'intelligence artificielle*, Bruxelles, Bruylant, 2025, pp. 71-75.
- BERTRAND B., « La politique de l'Union européenne en matière d'intelligence artificielle : entre approche sectorielle et transversale » *in Un droit de l'intelligence artificielle : entre règles sectorielles et régime général* (sous la dir. de C. CASTETS et J. EYNARD), Bruxelles, Bruylant, 2023, pp. 75-91.
- BERTHÉLÉMY C., « Mais que fait l'Europe ? », La *Chronique de la Ligue des droits humains asbl*, 2024, n° 208, pp. 17-19.
- BOCQUET N., « La Smart City à Bruxelles : quand 'intelligence' rime avec vidéosurveillance », *Brussels Studies*, 2021, p. 8-10.
- BORTELS H., KEYARTS D., VERRIJDT W. et DE GEYTER L., « Loi spéciale sur la Cour constitutionnelle : De la compétence de la Cour constitutionnelle », *in Focus sur le droit de la procédure devant la Cour constitutionnelle et le Conseil d'Etat*, Malines, Wolters Kluwer, 2024, pp. 15-16.
- BOURGOIN N., *La révolution sécuritaire (1976-2012)*, Nîmes, Champ Social Editions, 2013, p. 165.
- BOZZO-REY M., BRUNO-ERNST A. et WROBEL C., « Introduction », *in Reconnaissance faciale : Défis techniques, juridiques et éthiques* (sous la dir. de M. BOZZO-REY, A. BRUNO-ERNST et C. WROBEL), Paris, Editions Panthéon-Assas, 2024, p. 12.
- CALLENS S., *Démocratie et télésurveillance*, Villeneuve d'Ascq, Presses universitaires du Septentrion, 2002, p. 24.
- CAYOL A., « La protection des données personnelles de santé en France et en Europe par le Règlement Général sur la Protection des Données (RGPD) », *Droit, Santé et Société*, 2021, p. 53.
- CEYHAN A., « Editorial. Identifier et surveiller : les technologies de sécurité », *Cultures & Conflits*, 2006, pp. 7-9.

- CEYHAN A., « 'Acceptabilité' de la biométrie : linéaments d'un cadre analytique », *in L'identification biométrique : Champs, acteurs, enjeux et controverses* (sous la dir. de A. CEYHAN et P. PIAZZA), Paris, Editions de la maison des sciences de l'homme, 2011, p. 396.
- CHATELLIER R., « Des premières caméras à l'expérimentation des algorithmes : un panorama du développement territorial, technologique et de l'encadrement juridique de la vidéosurveillance », *Revue française d'administration publique*, 2024, pp. 223-227.
- CHATILA R. (e. a.), « Pourquoi la reconnaissance faciale, posturale et comportementale soulève-t-elle des questionnements éthiques » *in Pour une éthique du numérique* (sous la dir. de E. GERMAIN, C. KIRCHNER et C. TESSIER), Paris, Presses universitaires de France, 2022, pp. 211-212.
- COLFS B. et SMOOS S., « Des caméras ANPR au service de l'apaisement des quartiers », *Mouvement communal*, août-septembre, 2023, p. 56.
- COTON F., « Reconnaissance faciale dans l'espace public à des fins répressives : la CEDH ne condamne pas le principe, le Règlement IA l'encadre », *R.D.T.I.*, 2024, pp. 185-189.
- CROUZATIER-DURAND F., *Fiches de libertés publiques et droits fondamentaux*, Paris, Ellipses, 2021, p. 81.
- DAMBLY P. et BEELEN A., *(R)évolution de l'intelligence artificielle : vers un cadre juridique et technique de l'IA*, Limal, Anthémis, 2023, p. 381.
- DE BUISSERET HARDY E., « La reconnaissance faciale en procès ! », *La Chronique de la Ligue des droits humains* asbl, 2024, n° 208, pp. 3-5.
- DECHAMPS F. et ADAM M., « IA et reconnaissance faciale – Un outil prisé…mais à quel prix ? Analyse du cas Clearview AI », *D.P.O. News,* 2023, p. 21.
- DECROLY J., *Les jeux olympiques en valent-ils la chandelle ?*, Bruxelles, Editions de l'Université de Bruxelles, 2024, p. 185.
- DECROLY J., « Les jeux olympiques de Paris 2024 : cheval de Troie de la vidéosurveillance algorithmique », *La Chronique de la Ligue des droits humains asbl*, 2024, n° 208, pp. 14-15.
- DE KEERSMAECKER P. et DEBAILLEUL C., « The spatial distribution of open-street CCTV in the Brussels-Capital Region », *Brussels studies*, 2016, pp. 1-5.
- DENIAU M., « Entretien avec Drago : Les villes connectées fliquent l'espace public », *Silences*, 2020, pp. 46-48.
- DESVEAUD K., *L'intelligence artificielle décryptée : Comprendre les enjeux et les risques éthiques de l'IA pour mieux l'appréhender*, Caen, EMS Editions, 2024, p. 225.
- DE TERWAGNE C., « L'illégalité nuancée de la surveillance numérique : la réponse des juridictions belges et française à l'arrêt *La Quadrature du Net* de la Cour de justice de l'Union européenne », *Rev. Trim. D. H.*, 2022, pp. 4-9.

- DOCQUIR B., « Dompter les algorithmes ? Le nouveau règlement européen sur l'intelligence artificielle », *in Les platefromes numériques et l'intelligence artificielle* (sous la dir. de B. DOCQUIR), Limal, Anthemis, 2024, pp. 239-260.
- DUBUISSON F. , « La Cour européenne des droits de l'homme face à la surveillance de masse », obs. sous Cour eur. dr. h. (gde ch.), arrêt Big Brother Watch c. Royaume-Uni du 25 mai 2021, *Rev. trim. D. H.*, 2022, p. 129.
- DUMORTIER F., « L'accès aux données policières : un droit (in)direct susceptible de recours effectif », *DPO news*, 2023, p. 15.
- FARGE R., « Reconnaissance automatique des émotions, une valeur probante à haut risque », *La Chronique de la Ligue des droits humains* asbl, 2024, n° 208, p. 23.
- FODOR S., « Un cadre juridique pour une intelligence artificielle éthique : le règlement IA », *I2D – Information, données et documents*, 2024, pp. 79-81.
- FOEGLE J.-F., « La déconstruction de la vie privée des demandeurs d'asile », *Mémoires*, 2017, pp. 12-14.
- 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. 6.
- FORGET C., « L'effacement des données policières et judiciaires : un parcours du combattant ? », *e-legal Revue de droit et de criminologie de l'ULB*, 2022, pp. 3-22.
- FORTIN-TOURNÈS A.-L., « La reconnaissance faciale : une remise en question des champs de l'éthique et du politique ? », *in Reconnaissance faciale : Défis techniques, juridiques et éthiques* (sous la dir. de M. BOZZO-REY, A. BRUNO-ERNST et C. WROBEL), Paris, Editions Panthéon-Assas, 2024, p. 181.
- FRAENKEL B., « Un tournant biométrique ? » *in L'identification biométrique : champs, acteurs, enjeux et controverses* (sous la dir. de A. CEYAHN et P. PIAZZA), Paris, Editions de la maison des sciences de l'homme, 2011, pp. 418-419.
- GAÏA P., « La Charte des droits fondamentaux de l'Union européenne », *Revue française de droit constitutionnel*, 2004, p. 238.
- GILLIAUX P., « La force obligatoire de la Charte des droits fondamentaux de l'Union européenne », *Rev. trim. D. H.*, 2020, p. 78.
- GOFF T., « Le faux et coûteux miracle de la vidéosurveillance », *Après-demain,* 2010, pp. 28-30.
- GUILLARD et LOUIS V., « La loi « jeux olympiques » : l'arbre de l'expérimentation algorithmique cache la forêt de l'extension sécuritaire », *La Revue des droits de l'homme*, 2023, pp. 2-6.
- HARCOURT B.-E., *La société d'exposition*, Paris, Le Seuil, 2020, p. 77.

- HEILMANN E., « La vidéosurveillance, une réponse efficace à la criminalité ? », *Criminologie*, 2003, p. 101.
- HEILMANN E., « La vidéosurveillance, un mirage technologique et politique », *in La frénésie sécuritaire : retour à l'ordre et nouveau contrôle social* (sous la dir. de L. MUCCHIELLI), Paris, La Découverte, 2008, pp. 113-123.
- HEURTEBISE J.-Y., « Innovation, histoire et géopolitique en « Chine » : Revanche technologique, mimétisme impérialiste et techno-autoritarisme », *Monde chinois*, 2020, p. 94.
- KELLER P., « La perte de la face : réglementation et contestation de la surveillance biométrique », *in Reconnaissance faciale : Défis techniques, juridiques et éthiques* (sous la dir. de M. BOZZO-REY, A. BRUNO-ERNST et C. WROBEL), Paris, Editions Panthéon-Assas, 2024, pp. 82-88.
- KERNALEGENN T., « Identité », *in Dictionnaire encyclopédique de la décentralisation* (sous la dir. de N. KADA, R. PASQUIER, C. COURTECUISSE et V. AUBELLE), Boulogne-Billancourt, Berger-Levraut, 2017, p. 599.
- LAMBERT P., « L'utilisation de caméras par les services de police, dans le cadre de la loi sur la fonction de police du 5 août 1992 », *Postal Mémorialis*, 2020, p. 62.
- LAZERGES C., « Le droit à la sécurité a-t-il effacé le droit à la sûreté ? L'exemple de la loi 'Sécurité globale' », *La Revue des droits de l'homme*, 2021, p. 2.
- LECLERCQ-VANDELANNOITTE A., ISAAC H. et KALIKA M., *Travail à distance et e-management : organisation et contrôle en entreprise*, Paris, Dunod, 2013, p. 45.
- LÉGLISE P., « Le défi de l'encadrement juridique de l'IA : l'exemple de l'expérimentation de la vidéoprotection intelligente », *Servir*, 2024, p. 27.
- LEMAN-LANGLOIS S., *Sphères de surveillance*, Montréal, Les Presses de l'Université de Montréal, 2011, pp. 10-19.
- LEVY M., *Sortez vos données du frigo, une entreprise performante avec la Data et l'IA*, Paris, Dunod, 2021, p. 147.
- LHOUTELLIER P., « Données, technologies et systèmes d'information de sécurité : le contexte européen dans le temps de la présidence française de l'Union européenne », *Cahiers de la sécurité et de la justice*, 2022, p. 156.
- LOCHAK D., « L'image de l'étranger au prisme des lois sur l'immigration » *in Figures de l'étranger, quelles représentations pour quelles politique ?*, Paris, Gisti, 2013, pp. 36-37.
- MAKABA P., "L'incorportaion de la convention européenne des droits de l'homme dans l'ordre juridique britannique », *Rev. trim. dr. h.*, 2000, p. 19.
- MARGNYS J. , « La vie privée, pour quoi faire ? Exigence démocratique et reconnaissance faciale », *La Chronique de la Ligue des droits humains asbl*, 2024, n° 208, p. 10.

- MARGUENAUD J.-P. et ROETS D., « Droits de l'homme : jurisprudence de la CEDH », *Revue de science criminelle et de droit pénal comparé*, 2023, p. 630.
- MARISCAL V., « Compte-rendu de : Olivier Aïm, Les théories de la surveillance. Du panoptique aux Surveillances Studies », *La Nouvelle Revue du Travail,* 2021, p. 1.
- MERCIER J., « Sécuriser les JOP 2024 : quelle place pour la technologie ? », *Annales des Mines – Enjeux numériques*, 2024, p. 14-17.
- MICHEL A., « Révision de la loi caméras : précisions ou ambiguïtés pour l'installation et l'utilisation de caméras de surveillance ? », *J.T.*, 2019, pp. 149-160.
- MICKLITZ H.-W., « Règlement européen sur l'intelligence artificielle, normes harmonisées et effets externes », *Revue internationale de droit économique*, 2023, p. 75.
- MUCCHIELLI L., « A quoi sert la vidéosurveillance de l'espace public ? : Le cas français d'une petite ville 'exemplaire' », *Déviance et société*, 2016, p. 45.
- MUCCHIELLI L., « La vidéosurveillance réduit-elle la criminalité ? » *in L'enseignement universitaire en milieu carcéral : Expériences comparées entre la France et l'Italie* (sous la dir. de P. PACINI VOLPE), Nîmes, Champ social, 2021, pp. 256-257.
- NUYTTEN M., « De Europese Commissie onthult een nieuwe reeks voorstellen om artificielë intelligentie te reguleren», *T.B.H.*, 2021/5, p. 662.
- O'FLAHERTY M., « Facial recognition technology and fundamental rights", *E.D.P.L.*, 2020, p. 171.
- Organisation de coopération et de développement économique, *L'intelligence artificielle dans la société*, Paris, Editions de l'OCDE, 2019, p. 78.
- PARSA S. et VOLCANSEK E., « L'impact de la protection des données sur la surveillance de masse : examen de l'arrêt Big Brother Watch et autres c. Royaume-Uni de la Cour européenne des droits de l'homme », *DPO news*, 2022, pp. 8 - 13.
- PEETERS B., « Het gebruik van camera's met gezichtsherkenning : perspectieven na het proefproject in Zaventem », *Politie & Recht*, 2020, pp. 155-160.
- PEYROU S., « Nouvelles technologies, sécurité et protection des données à caractère personnel : un cadre juridique européen à la hauteur des enjeux ? », *Cahiers de la sécurité et de la justice*, 2022, pp. 189-195.
- PREUSS-LAUSSINOTTE S., « Bases de données personnelles et politiques de sécurité : une protection illusoire ? », *Cultures & Conflits*, 2006, pp. 1-10.
- PREUSS-LAUSSINOTTE S., « L'élargissement problématique de l'accès aux bases de données européennes en matière de sécurité », *Cultures & Conflits*, 2009, p. 83.
- RENUCCI J.-F. et RENUCCI A., *Droit et protection des données à caractère personnel, droit européen : RGPD, Convention européenne des droits de l'homme*, Paris, LGDJ, 2022, p. 197.

- REYHAN D., « Génocide Ouïghour : cheminement d'un projet colonial », *Monde chinois*, 2021, p. 19.
- ROSOUX G., « Panorama de la protection juridictionnelle nationale des droits fondamentaux : qui est le juge des droits fondamentaux en Belgique ? », *in Contentieux des droits fondamentaux* (sous la dir. de F. KRENC, F. BOUHON et C. DEPREZ), Limal, Anthemis, 2021, p. 9.
- ROUSSET F., « Biométrie et sécurité des installations sensibles », *Sécurité et stratégie*, 2018, pp. 26-27.
- ROUSVOAL L., « L'accès des services répressifs aux données de migrants et réfugiés présentes dans le fichier Eurodac » *in Les données numériques des migrants et des réfugiés sous l'angle du droit européen* (sous la dir. de S. TURGIS), Rennes, Presses universitaires de Rennes, 2020, p. 82.
- SALMONA L., *Politiser les cyberviolences – Une lecture intersectionnelle des inégalités de genre sur internet*, Paris, Le Cavalier Bleu, 2023, p. 30.
- SOENEN P., PARSA S. et RAGHENO N., « News », *DPO-pro mag*, 2023, p. 8.
- STROWEL A., « L'intelligence artificielle : vers une régulation européenne par la gestion des risque », *Les pages : obligations, contrats et responsabilités*, 2021, p. 1.
- SZYMCZAK D., « Chronique de jurisprudence de la Cour européenne des droits de l'homme (2023) », *Rev. trim. D. H.*, 2024, p. 378.
- TETERINA V., *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 ?* (multig.), Mémoire de master de la faculté de droit et de criminologie, Louvain-la-Neuve, Université catholique de Louvain, 2023.
- TRÉGUER F., *Technopolice : La surveillance policière à l'ère de l'intelligence artificielle*, Quimperlé, Editions Divergences, 2024, p. 84.
- TRSTENJAK M., « Analyse des bas à sable réglementaires d'IA dans l'AI Act », *R.P.I.N.*, 2024/19, pp. 11-12.
- TRULLEMANS J., « Evaluation de la loi du 10 avril 1990 réglementant la sécurité privée et particulière : Compétences générales et situationnelles », *Postal Mémorialis*, 2023, pp. 126-129.
- TRULLEMANS J., « Plan national de sécurité : Groupes (clusters) de phénomènes de sécurité », *Postal Mémorialis*, 2018, pp. 165-166.
- VAAL E., « Boete voor Clearview AI », *Computerrecht*, 2024, p. 426.
- VALDELIEVRE G., "La sécurité juridique – Le point de vue de l'avocat », *Titre VII*, 2020/2, p. 13.

- VANLEEUW R., « Clearview AI : COC-rapport vernietigend voor Belgische Federale Politie », *Computerrecht*, 2022, p. 251.
- VAN ONACKER S., *Le recours à la technologie de reconnaissance faciale dans l'espace public : quel impact sur le droit au respect de la vie privée ?* (multig.), Mémoire de master de la faculté de droit et de criminologie, Louvain-la -Neuve, Université catholique de Louvain, 2024.
- VERDOODT V., "The regulation of artificial intelligence", *in An Introduction to Law & Technology* (sous la dir. de E. Lievens, C. Vander Maelen et S. Verschaeve), Gand, Owl Press Legal, 2024, p. 432.
- VOIGT P. et HULLEN N., *The EU AI Act : Answers to frequently asked questions*, Berlin, Springer, 2024, p. 45.
- WAVREILLE A., « Reconnaissance faciale : fuyez, vous êtes filmé.es … et identifié.es », *La Chronique de la Ligue des droits humains asbl*, 2023, n° 203, p. 5.

Sources électroniques

Organisations et associations

- Amnesty International France, « Les technologies automatisées et l'avenir de la forteresse Europe », 2019, https://www.amnesty.org/fr/latest/news/2019/03/automated-technologies-and-the-future-of-fortress-europe/ (date de dernière consultation le 9 avril 2025).
- Amnesty International France, « Des entreprises de l'UE vendent des outils de surveillance à des responsables d'atteintes aux droits humains en Chine », 2020, https://www.amnesty.org/fr/latest/press-release/2020/09/eu-surveillance-sales-china-human-rights-abusers/ (date de dernière consultation : 11 avril 2025).
- Amnesty International, « Apartheid automatisé : Comment la reconnaissance faciale fragmente, ségrègue et contrôle les Palestiniens et les Palestiniennes dans les TPO », 2023, pp. 7-77, https://www.amnesty.org/fr/documents/mde15/6701/2023/fr/ (date de dernière consultation : 17 avril 2025).
- Amnesty International France, « J.O. 2024 : Pourquoi la vidéosurveillance algorithmique pose problème », 2024, https://www.amnesty.fr/liberte-d-expression/actualites/pourquoi-la-videosurveillance-algorithmique-pose-probleme-cameras-technologies (date de dernière consultation : 28 mars 2025).
- Amnesty International France, « Cinq outils numériques utilisés aux frontières contre les personnes exilées », 2024, https://www.amnesty.fr/refugies-et-migrants/actualites/technologies-et-reconnaissance-faciale-aux-frontieres-la-derive-contre-les-personnes-exilees (date de dernière consultation : 9 avril 2025).

- Amnesty International France, « Voici comment le gouvernement a prolongé la vidéosurveillance algorithmique », 2025, https://www.amnesty.fr/actualites/voici-comment-le-gouvernement-a-prolonge-la-videosurveillance-algorithmique (date de dernière consultation : 1er avril 2025).
- La Quadrature du net, « VSA jusqu'en 2027 : quand le gouvernement ose tout », 7 février 2025, https://www.laquadrature.net/2025/02/07/vsa-jusquen-2027-quand-le-gouvernement-ose-tout/ (date de dernière consultation : 1er avril 2025).
- La Quadrature du Net, « Nous », https://www.laquadrature.net/nous/ (date de dernière consultation : 26 mars 2025).
- Liga voor mensen rechten, « Waarom er nood is aan een Belgisch verbod op gezichtsherkenningstechnologie in de openbare ruimte », https://mensenrechten.be/pagina/nota-gezichtsherkenning (date de dernière consultation : 16 avril 2025).
- Ligue des droits humains, « Actions en justice », https://www.liguedh.be/en-action/actions-en-justice/ (date de dernière consultation : 8 mai 2025).
- Ligue des droits humains, « 'On vous voit' : l'utilisation de la reconnaissance faciale et les questions de surveillance au centre du procès fictif de la Ligue des droits humains », 2024, https://www.liguedh.be/on-vous-voit-lutilisation-de-la-reconnaissance-faciale-et-les-questions-de-surveillance-au-centre-du-proces-fictif-de-la-ligue-des-droits-humains/ (date de dernière consultation : 17 mars 2025).
- Ligue des droits humains, « Protectmyface », https://www.liguedh.be/une-petition-pour-interdire-la-reconnaissance-faciale-dans-lespace-public-bruxellois-2/ (date de dernière consultation : 9 avril 2025).
- Ligue des droits humains, « Accord 'Arizona' : recul préoccupant pour les droits sociaux et droits des étranger.ères et tournant sécuritaire confirmé », 2025, https://www.liguedh.be/accord-arizona-recul-preoccupant-pour-les-droits-sociaux-et-droits-des-etranger%c2%b7eres-et-tournant-securitaire-confirme/ (date de dernière consultation : 15 avril 2025).
- Ligue des droits humains, « Reconnaissance faciale : 'La Belgique doit interdire totalement cette technologie de surveillance' », 31 janvier 2025, https://www.liguedh.be/reconnaissance-faciale-la-belgique-doit-interdire-totalement-cette-technologie-de-surveillance/ (date de dernière consultation : 30 mars 2025).
- Ligue des droits humains France, « Les frontières (numériques) de l'Europe doivent tomber : mettre fin à l'expansion de la base de données eurodac de l'UE », 2023, https://www.ldh-france.org/la-societe-civile-demande-quil-soit-mis-fin-a-lexpansion-de-la-base-de-donnees-eurodac-de-lue/ (date de dernière consultation : 2 avril 2025).

- Podcast « De quels droits on se chauffe. Fuyez, vous êtes identifié.es ! – épisode 1 » - Ligue des droits humains.

Institutions européennes

- Commission européenne, « Communiqué de presse : Entrée en vigueur du règlement européen sur l'intelligence artificielle », 1er août 2024, https://ec.europa.eu/commission/presscorner/api/files/document/print/fr/ip_24_4123/IP_24_4123_FR.pdf (date de dernière consultation : 24 mars 2025).
- Commission européenne, « Intelligence artificielle – Questions et réponses », 1er août 2024, https://ec.europa.eu/commission/presscorner/detail/fr/qanda_21_1683 (date de dernière consultation : 30 mars 2025).
- Commission européenne, « Livre blanc : Intelligence artificielle, une approche européenne axée sur l'excellence et la confiance », COM/2020/65 final, p. 11. https://commission.europa.eu/document/download/ (date de dernière consultation : 28 mars 2025).
- Conseil européen, « Réunion du Conseil européen (19 octobre 2017) – Conclusions, EUCO 14/17 », 2017, p. 7, https://data.consilium.europa.eu/doc/document/ST-14-2017-INIT/fr/pdf, (date de dernière consultation : 26 mars 2025).
- Conseil de l'Europe, « Le rapporteur du Congrès est profondément préoccupé par l'amendement constitutionnel en Hongrie », 16 avril 2025, https://www.coe.int/fr/web/portal/-/-we-should-all-be-proud-of-pride-congress-rapporteur-deeply-concerned-by-constitutional-amendment-in-hungary (date de dernière consultation : 5 mai 2025).
- E.D.P.B., "Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement", 26 avril 2023, p. 15, https://www.edpb.europa.eu/system/files/2023-05/edpb_guidelines_202304_frtlawenforcement_v2_en.pdf (date de dernière consultation : 9 mai 2025).
- F.R.A., « Under watchful eyes : biometrics, EU IT systems and fundamental rights », *Office des publications de l'Union européenne*, 2018, p. 17, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-biometrics-fundamental-rights-eu_en.pdf (date de dernière consultation le 1er avril 2025).
- F.R.A. « Technologie de reconnaissance faciale : considérations relatives aux droits fondamentaux dans le contexte de l'application de la loi », *Office des publications de l'Union européenne*, 2020, pp. 12-33, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper_fr.pdf (date de dernière consultation : 21 mars 2025).

- F.R.A., « Bien préparer l'avenir : l'intelligence artificielle et les droits fondamentaux », *Office des publications de l'Union européenne*, 2021, pp. 5-10, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2021-artificial-intelligence-summary_fr.pdf (date de dernière consultation : 18 mars 2025).
- MADIEGA T. et MILDEBRATH H., « Réglementation de la reconnaissance faciale au sein de l'Union européenne », *Service de recherche du Parlement européen*, 2021, p. 18, https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_FR.pdf (date de dernière consultation : 28 mars 2025).
- Parlement européen, « Loi sur l'IA de l'UE : première réglementation de l'intelligence artificielle », 27 mars 2024, https://www.europarl.europa.eu/ (date de dernière consultation : 28 mars 2025).

Médias

- DROESBEKE L., « Investigation : Clearview AI, quand la reconnaissance faciale porte atteinte à la vie privée », R.T.B.F., 13 juin 2023, https://www.rtbf.be/article/investigation-clearview-ai-quand-la-reconnaissance-faciale-porte-atteinte-a-la-vie-privee-11212380 (date de dernière consultation : 22 mars 2025).
- MACMILLAN D., OVALLE D. et SCHAFFER A., « Arrester by AI : Police ignore standards after facial recognition matches", *The Washington Post*, 2025, https://www.washingtonpost.com/business/interactive/2025/police-artificial-intelligence-facial-recognition/ (date de dernière consultation : 6 avril 2025).
- M. P., « La Hongrie de Viktor Orban interdit la marche des fiertés et va utiliser la reconnaissance faciale pour cibler les participants », Le Parisien, 2025, https://www.leparisien.fr/societe/la-hongrie-de-viktor-orban-interdit-la-marche-des-fiertes-et-va-utiliser-la-reconnaissance-faciale-pour-cibler-les-participants-19-03-2025-WNQ72DER4JETZKJWA2MUJVLWTU.php (date de dernière consultation : 15 mars 2025).
- NOIRFALISSE Q., « Courtrai, reconnaissance faciale dans le viseur ? », Médor, 23 décembre 2021, https://medor.coop/hypersurveillance-belgique-surveillance-privacy/police-justice-bng/episodes/courtrai-reconnaissance-faciale-dans-le-viseur-camera-criminalite-videosurveillance-briefcam-biometrie/?full=1 (date de dernière consultation : 25 mars 2025).
- X. « Hongrie : des milliers de manifestants protestent à Budapest contre une loi interdisant la Gay Pride », RTBF, 2025, https://www.rtbf.be/article/hongrie-des-milliers-de-manifestants-protestent-a-budapest-contre-une-loi-interdisant-la-gay-pride-11526924 (date de dernière consultation : 15 mars 2025).

- X., « Histoire belge : les caméras intelligentes qui vont sanctionner le GSM au volant sont… illégales », RTL Info, 2022, https://www.rtl.be/actu/belgique/societe/histoire-belge-les-cameras-intelligentes-qui-vont-sanctionner-le-gsm-au-volant/2022-11-05/article/499617 (date de dernière consultation : 10 mars 2025).

Divers

- Accord de coalition fédérale 2025-2029, p. 109, https://www.belgium.be/sites/default/files/resources/publication/files/Accord_gouvernemental-Bart_De_Wever_fr.pdf (date de dernière consultation : 17 mars 2025).
- Assemblée générale des Nations Unies « Conseil des droits de l'homme : Surveillance et droits de l'homme : Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression », 2021, https://documents.un.org/doc/undoc/gen/g19/148/77/pdf/g1914877.pdf (date de dernière consultation : 5 avril 2025).
- C.N.I.L., « Reconnaissance faciale : pour un débat à la hauteur des enjeux », 2019, pp. 5-6, https://www.cnil.fr/fr/reconnaissance-faciale-pour-un-debat-la-hauteur-des-enjeux (date de dernière consultation : 1er avril 2025).
- C.N.I.L., « Les caméras 'augmentées' ou algorithmiques dans l'espace public », 2024, https://www.cnil.fr/fr/cameras-augmentees-espaces-publics (date de dernière consultation : 25 février 2025).
- Commissaire à la protection des données et à la liberté d'information de Hambourg, « Evaluation juridique en matière de protection des données de l'utilisation d'un logiciel de reconnaissance faciale par la police de Hambourg aux fins d'élucidation d'infractions en lien avec le sommet du G20 », 31 août 2018, p. 2, https://datenschutz-hamburg.de/fileadmin/user_upload/HmbBfDI/Datenschutz/Informationen/Pruefbericht_Gesichtserkenungssoftware.pdf (date de dernière consultation : 3 mai 2025).
- Défenseur des droits, « Technologies biométriques : l'impératif respect des droits fondamentaux », 2021, p. 14, https://www.defenseurdesdroits.fr/rapport-technologies-biometriques-limperatif-respect-des-droits-fondamentaux-274 (date de dernière consultation : 1er avril 2025).
- DUBOIS C., « Note d'analyse 9-24 du Centre d'études Jacques Georgin : Vers une législation de la reconnaissance faciale en Belgique ? Enjeux et stratégies », 20 septembre 2024, https://www.cejg.be/wp-content/uploads/2025/01/Note-danalyse-9-24-du-CeG-Enjeux-lies-au-deploiement-de-la-reconnaissance-faciale-en-Belgique.pdf (date de dernière consultation : 25 mars 2025).

- E.D.R.I., « Ban Biometric Mass Surveillance : A set of fundamental rights demands for the European Commission and EU Member States », Bruxelles, 2020, pp. 21-23, https://edri.org/wp-content/uploads/2020/05/Paper-Ban-Biometric-Mass-Surveillance.pdf (date de dernière consultation : 25 mars 2025)
- E.D.R.I., « EDRi and Reclaim Your Face campaign recognised as Europe AI Policy leaders", 2024, https://edri.org/our-work/edri-reclaim-your-face-campaign-awarded/ (date de dernière consultation : 10 avril 2025).
- E.D.R.I., « How to fight Biometric Mass Surveillance after the AI Act : a legal and practical guide », 2024, https://edri.org/our-work/how-to-fight-biometric-mass-surveillance-after-the-ai-act-a-legal-and-practical-guide/ (date de dernière consultation : 11 avril 2025).
- MyData, « Votre plateforme sur la transparence des données fédérales », https://mydata.belgium.be/fr/ (date dernière consultation : 25 février 2025).
- NLets, « Privacy impact assessment report for the utilization of recognition technologies to identify subjects in the field », 2011, p. 19, https://www.eff.org/files/2013/11/07/09_-_facial_recognition_pia_report_final_v2_2.pdf (date de dernière consultation : 25 mars 2025
- Organe de contrôle de l'information judiciaire, « Législation relative à l'usage de caméras », https://www.organedecontrole.be/services-de-police/l%C3%A9gislation-relative-%C3%A0-lusage-de-cam%C3%A9ras (date de dernière consultation : 2 mars 2025).
- Organe de contrôle de l'information policière, « Avis relatif à la proposition de loi modifiant l'arrêté royal du 18 décembre 2002 en ce qui concerne l'usage du téléphone portable au volant », pp. 2-7, https://www.organedecontrole.be/files/DA210003-FR.pdf (date de dernière consultation : 15 mars 2025).
- Organe de contrôle de l'information policière, « 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 à l'aéroport national de Zaventem (DIO19005) », p.4, https://www.organedecontrole.be/files/DIO19005_Contr%C3%B4le_LPABRUNAT_Reconnaissance_Faciale_Publique_F.PDF , p.4 (date de dernière consultation : 17 mars 2025).
- Organe de contrôle de l'information policière, « Avis de l'organe de contrôle de l'information policière relatif à une proposition de résokution 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 », 24 janvier 2022, https://www.organedecontrole.be/files/DA210029_Avis_F.pdf (date de dernière consultation le 16 mars 2025).

- Organe de contrôle de l'information policière, « 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) », 2022, p. 4, https://www.organedecontrole.be/files/DIO21006_Rapport_Contrôle_Clearview_F_00050441.pdf (date de dernière consultation : 22 mars 2025).
- POUGET H., « Contexte institutionnel », Future of Life Institute, https://artificialintelligenceact.eu/fr/contexte/ (date de dernière consultation : 29 mars 2025).
- The Greens/EFA, « Biometric & behavioural mass surveillance in EU member states », pp. 50-98, https://extranet.greens-efa.eu/public/media/file/1/7297 (date de dernière consultation 21 mars 2025).
- Von Der Leyen U. « Une Union plus ambitieuse, Mon programme pour l'Europe : orientations politiques pour la prochaine commission européenne 2019-2024», https://commission.europa.eu/document/download/063d44e9-04ed-4033-acf9-639ecb187e87_fr?filename=political-guidelines-next-commission_fr.pdf (date de dernière consultation : 27 mars 2025).
- X., « Briefcam », Technopolice, https://technopolice.fr/briefcam/ (date de dernière consultation : 21 mars 2025).
- X. « What is video analytics », BriefCam, https://www.briefcam.com/technology/video-analytics/ (date de dernière consultation : 21 mars 2025).
- X., « Chronologie historique », Future of Life Institute, https://artificialintelligenceact.eu/fr/developpements/ (dernière consultation : 29 mars 2025).
- X. « High level summary of the AI Act", Future of Life Institute, 27 février 2024, https://artificialintelligenceact.eu/high-level-summary/ (date de dernière consultation : 30 mars 2025).

Autre :

- Open AI, Chat GPT 4-o, https://chatgpt.com/ (à des fins de correction orthographique et grammaticale).
- Entretien avec Rémy Farge, formateur à la Ligue des droits humains, tenu le 24 mars 2025.

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