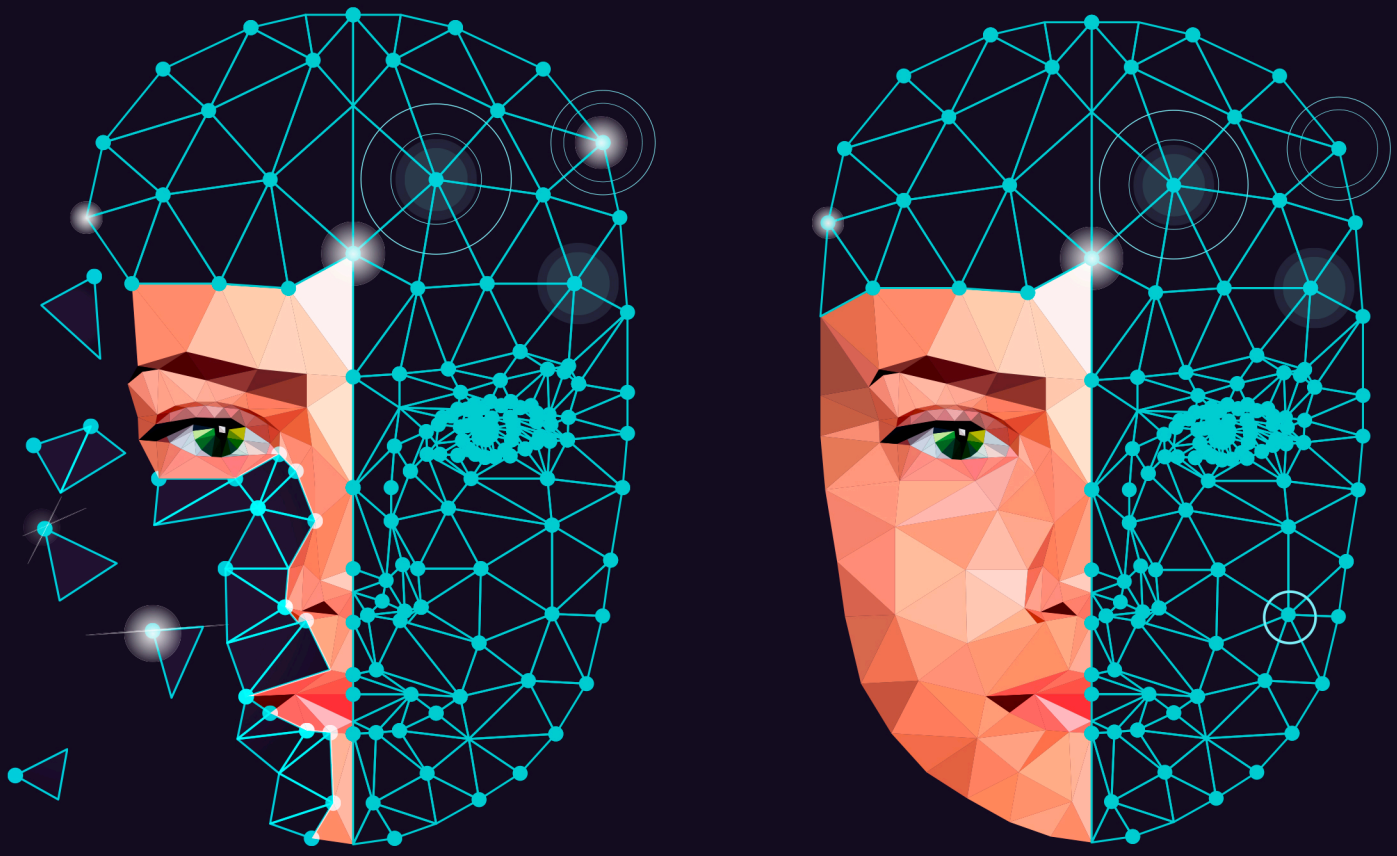
La Reconnaissance Faciale dans l'espace public - Une cartographie européenne

Caroline Lequesne Roth, Mehdi Kimri, Pierre Legros

LA RECONNAISSANCE FACIALE DANS L'ESPACE PUBLIC

Une cartographie juridique européenne



Rapport de la Fablex DL4T

Avril 2020

Sous la direction de Caroline LEQUESNE ROTH

Avec les contributions de : Jérémie CAFFIN, Mehdi KIMRI, Maxime KUBIAK, Clara LACOUR, Pierre LEGROS, Marion LEMOS

LA RECONNAISSANCE FACIALE DANS L'ESPACE PUBLIC

Une cartographie juridique européenne

Rapport de la Fablex DL4T

Avril 2020

Sous la direction de Caroline Lequesne Roth

Avec les contributions de : Jérémie Caffin, Mehdi Kimri, Maxime Kubiak, Clara Lacour, Pierre Legros, Marion Lemos

«Les personnes ne sont pas l'une devant l'autre, simplement elles sont les unes avec les autres autour de quelque chose. Le prochain, c'est le complice ».

Emmanuel Levinas
De l'existence à l'existant, 1978.

Remerciements

Ce travail n'aurait pu voir le jour sans le soutien de notre institution. Nous remercions Université Côte d'Azur, et plus particulièrement les équipes de l'Idex UCA Jedi, ainsi que la Faculté de Droit et Science politique de Nice, pour la confiance et le soutien apportés à la Fablex.

Nous adressons nos remerciements à Julie Charpenet, coordinatrice de la Fablex-DL4T, pour son écoute et ses conseils auprès des étudiants, ainsi que Marion Musso pour sa grande disponibilité.

Nous adressons également nos remerciements aux acteurs de terrain. Ils ont su nous accorder de leur précieux temps, et un éclairage indispensable à la compréhension de la technologie et ses enjeux :

- Monsieur Jonathan J. Attia, chercheur associé au GREDEG UMR 7321 CNRS pour son séminaire sur la question ;
- Madame Marine Brenier, Députée des Alpes Maritimes ;
- Madame Sandra Bertin, Directrice de la Police Municipale de Nice, ainsi qu'à l'ensemble du personnel du Centre de Supervision Urbain de Nice, en particulier Monsieur Gregory Pezet, Directeur du Centre ;
- Monsieur le Professeur Jean-Marc Ogier, Président de l'Université de la Rochelle et Directeur du Laboratoire Informatique, Image et Interaction (L3i) ;
- Sébastien Viano, Directeur Europe et Financements Extérieurs, DGA Attractivité Economique, Innovation, Tourisme et International de la Métropole Nice Côte d'Azur.

Nous remercions les acteurs associatifs parmi lesquels la section niçoise de la Ligue de Droits de l'Homme, tout spécifiquement Monsieur Henri Busquet pour nos précieux échanges ainsi que la Quadrature du Net à travers les personnes de Monsieur Martin Drago et Monsieur Arthur Messaud.

Merci également aux fabricateurs de Master I : Lena, Léonie, Lucas et Tommy pour leur aide logistique précieuse.

Nous remercions enfin Marina Teller, Stéphane Prévost et Sumi Saint-Auguste, pour leur bienveillance, leurs encouragements et leur soutien.

Qu'il nous soit permis, par le présent rapport, d'apporter notre modeste contribution au débat sur la reconnaissance faciale ô combien important pour nos sociétés.

Table des abréviations

AEPD	*Agencia Española de Protección de Datos*
AIPD	Analyse d'Impact relative à la Protection des Données
CBP	*College bescherming persoonsgegevens*
CEDH	Convention Européenne des Droits de l'Homme
CNIL	Commission Nationale de l'Informatique et des Libertés
CSI	Code de la Sécurité Intérieure
BDSV	*Bundesvereinigung Deutscher Stahlrecycling und Entsorgungsunternehmen*
EES	*Entry - Exit System*
G29	Groupe de travail « article 29»
ICO	*Information Commissioner's Office*
LIL	Loi relative à l'Informatique, aux fichiers et aux Libertés
Met	Police métropolitaine de Londres
PARAFE	Passage Automatisé Rapide Aux Frontières Extérieures
RGPD	Règlement Général sur la Protection des Données
RWDM	*Racing White Daring Molenbeek*
SARI	Sistema Automatico di Riconoscimento Immagini
SIS	*Schengen Information System*
TA	Tribunal Administratif
UE	Union Européenne

SOMMAIRE

INTRODUCTION

L'État de surveillance technologique. L'année 2019 inscrit l'État de surveillance dans la modernité[1]. Le Panopticon, renforcé d'un arsenal technologique dernier cri, équipe peu à peu nos villes dans la promesse dystopique de l'« intelligence » technologique. Souriez, vous êtes filmés, traqués, profilés. Le phénomène n'est évidemment pas nouveau, mais se distingue par son ampleur : il est tout à la fois global et multidimensionnel. Global, car il prend forme, indifféremment, dans les régimes démocratiques et autoritaires, de Londres à Nairobi. Multidimensionnel, il l'est encore, car il prend racine dans les structures profondes de nos sociétés et transcende les frontières du public et du privé. Shoshana Zuboff décrit cette intrication dans un ouvrage qui s'imposa en quelques semaines comme la référence d'une génération : le « capitalisme de surveillance »[2]. Elle analyse comment l'appareillage technologique sécuritaire traduit l'expérience humaine en données informatiques pour orienter nos comportements de consommateur et de citoyen.

Reconnaissance faciale – Une définition. Du drone aux micros, en passant par les caméras corporelles, les dispositifs technologiques sécuritaires sont nombreux. Le présent rapport intéresse toutefois une technologie bien spécifique, qui alimente espoirs, craintes et fantasmes dans le débat public : la technologie de reconnaissance faciale. La reconnaissance faciale est une technique qui permet, à partir des traits de visage, d'authentifier une personne - vérifier que celle-ci est bien celle qu'elle prétend être – ou l'identifier, c'est-à-dire la retrouver au sein d'un groupe d'individus, dans un lieu, une image ou une base de données. Ces deux applications reposent sur un modèle probabiliste visant à évaluer la correspondance entre un visage et le gabarit numérique de celui-ci[3].

Traitement des données biométriques. La reconnaissance faciale est, de ce fait, indissociable d'un traitement de données biométriques : ce sont les caractéristiques physiques du visage qui permettent de « reconnaître » la personne. L'exploitation de ces données distingue la technologie des autres dispositifs d'enregistrement de vidéos, tels que les caméras de vidéo protection ou de surveillance. Bien que formant un même « continuum technologique »[4], ils permettent seulement de filmer les personnes.

Les usages de la reconnaissance faciale dans l'espace public. La technologie de reconnaissance faciale est mobilisée – ou susceptible de l'être – à diverses fins, des usages « récréatifs » et privés, au maintien de l'ordre public. Le présent rapport intéresse plus spécifiquement les usages de la technologie dans l'espace public. Celui-ci est compris au sens large, comme tout lieu de passage ou de rassemblement accessible à tous, indépendamment de la qualité du domaine (public ou privé). Si les autorités publiques apparaissent, dans ce cadre, comme les principaux responsables de traitement, les expérimentations constituent le terrain privilégié des collaborations entre acteurs publics et privés. La porosité des domaines apparaît ici particulièrement prégnante.

Les enjeux. La technologie n'emporte pas le consensus et alimente les suspicions. Si le débat public est engagé dans de nombreux États – et ce, au-delà des frontières européennes[5] -, les usages appropriés (**efficacité**), légaux (**légalité**), et acceptables (**légitimité**) doivent encore être déterminés. Ils appelleront inévitablement des compromis entre sécurité et libertés, qui définiront, plus largement, le cadre des technologies de surveillance. Dans cette perspective, et au regard du potentiel liberticide de la technologie, plusieurs points de vigilance doivent être observés.

1 S. Feldstein, "The Global Expansion of AI Surveillance", *Paper for Carnegie endowment for international peace*, September 17, 2019
https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847

2 S. Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, Profile Books Édition, Main, January 2019, 705 p.

3 Notons en outre que les dispositifs sont technologiquement aussi nombreux que les entreprises qui les fournissent.

4 Selon l'expression à laquelle recours la CNIL française dans ses publications. Voy. par exemple : CNIL, *Reconnaissance Faciale : pour un débat à la hauteur des enjeux*, 15 novembre 2019, p.4.[en ligne] https://www.cnil.fr/sites/default/files/atoms/files/reconnaissance_faciale.pdf

5 Particulièrement dans les villes et les États américains.

⇨ ***La sensibilité des données utilisées***. La donnée biométrique est « immuable » : elle ne dépend pas de la volonté propre de l'individu, elle lui est attachée sans que celui-ci ne puisse s'en défaire - à l'exception de se grimer, de recourir à la chirurgie ou de porter des artifices.
Le scandale survenu à la suite des révélations du New York Times concernant la société Clearview AI[6] révèle la vulnérabilité à laquelle le déploiement des dispositifs expose ces données. La start-up américaine a constitué, à partir des réseaux sociaux, une base de données biométriques permettant l'identification des individus. Plus de trois milliards de profils y ont été clandestinement – c'est à dire sans le consentement des individus – regroupés. Ils ont été indistinctement vendus aux autorités de police, aux universités, aux acteurs privés et autres milliardaires à l'échelon mondial, et ce compris sur le territoire européen[7].

⇨ ***Surveillance généralisée***. Comme le souligne la Commission Nationale de l'Informatique et des Libertés française, l'adoption de la reconnaissance faciale dans l'espace public conduirait à un « changement de paradigme » : « d'une surveillance ciblée de certains individus », la technologie offre la perspective « d'une surveillance de tous aux fins d'en identifier certains »[8]. Le caractère ubiquitaire de la technologie, qui échappe à tout contact avec les individus, renforce en outre le phénomène.
Cette évolution, inquiétante, n'est pas acceptable en tant que tel dans un régime démocratique. D'une part, la liberté de se mouvoir anonymement dans l'espace public ne saurait être entravée et conditionnée par la lecture « technologique » de nos comportements ; la surveillance généralisée des individus est manifestement disproportionnée au regard de l'objectif de maintien de l'ordre public poursuivi. D'autre part, elle ne peut conduire ni reposer sur un « fichage » généralisé des individus. Les exemples étrangers traduisent très concrètement cette menace : oppression des manifestants hongkongais et russes, de la minorité ouïgoure en Chine, traque des Palestiniens en Cisjordanie. Outre le ciblage politique, celui des migrants ou des délinquants condamnés apparaît tout aussi contraire aux principes démocratiques.

⇨ ***Failles techniques***. Les failles techniques sont encore nombreuses. Parmi celles-ci, les biais algorithmiques conduisent à exacerber - voir créer - des situations discriminantes. Rappelons que la technologie repose sur des estimations statistiques dont la pertinence peut varier en fonction de l'environnement (angles, lumière, résolution d'image), de l'âge, de la couleur de peau ou du sexe des personnes. Comme l'ont établi diverses études[9], le risque de faux positifs et de faux négatifs est important. Une identification erronée peut emporter des conséquences juridiques, sociales, et psychologiques non négligeables pour les individus ; elle est en outre susceptible de nuire à la cohésion sociétale en stigmatisant certains groupes où les erreurs sont plus nombreuses[10]. Aux États-Unis, les risques qui en résultent pour les autorités de police – une dégradation des relations avec les administrés - constituent l'une des principales critiques adressées aux dispositifs.

Une cartographie européenne. Phénomène global, la technologie s'est emparée du débat public national et européen suscitant, de la part des pouvoirs publics, des prises de position attentistes. De nombreux gouvernements encouragent avec constance la multiplication des expérimentations en vue d'offrir, à leurs in-

---

6 K. Hill, "The Secretive Company That Might End Privacy as We Know It", *New York Times*, Jan. 18, 2020, [en ligne] https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html

7 S. Stolton, Bruxelles se penche sur le scandale Clearview AI sur la reconnaissance faciale, Euractiv, 13 février 2020 [en ligne] www.euractiv.fr/section/economie/news/after-clearview-ai-scandal-commission-in-close-contact-with-eu-data-authorities/

8 CNIL, *Reconnaissance Faciale : pour un débat à la hauteur des enjeux*, précédemment cité, p.7.

9 J. Buolamwini & T. Gebru, «Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification", Conference on Fairness, Accountability, and Transparency, *Proceedings of Machine Learning Research* 81:1–15, 2018; P. Grother, M. Ngan, K. Hanaoka, "Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects", NISTIR 8280, U.S. Department of Commerce, December 2019, [en ligne] https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf ; CNIL, *Reconnaissance Faciale : pour un débat à la hauteur des enjeux*, précédemment cité, p.8.

10 Notamment pour les personnes de couleur comme en témoigne les travaux ci-dessus, *Ibidem.*

dustriels, les terrains d'application indispensables à la formation de champions nationaux. Si la Commission européenne plaide pour l'uniformisation des usages circonstanciés dans le respect des droits fondamentaux et de la protection des données[11], elle identifie l'urgence dans le « débat » : interdiction et moratoire, un temps envisagés, sur le modèle de la loi californienne[12], ne sont pas à l'agenda.

Le présent rapport s'inscrit dans ce contexte. Il vise à apporter un éclairage sur l'état du droit, les prises de position des autorités nationales compétentes, et les expérimentations nationales conduites. Ce travail a notamment pour objectif d'identifier les points de convergence entre les États et d'interroger l'existence d'une voix commune.

Cette étude n'est pas exhaustive. Nous avons choisi d'étudier un échantillon de 9 pays : **l'Allemagne, la Belgique, l'Espagne, la France, l'Italie, les Pays-Bas, la République tchèque, le Royaume-Uni et la Suède**. Nous apportons également des informations relatives aux expérimentations conduites au **Danemark, en Finlande et en Slovénie**. Ce choix s'est fondé sur les données nationales accessibles, au regard des langues maîtrisées par les auteurs de l'étude.

Méthode. Pour conduire ce travail, différentes méthodes ont été mises en œuvre :

- La méthode analytique a été privilégiée pour étudier les textes produits (législation, positions des autorités compétentes, et plus rarement jurisprudences) ; nous y recourons pour l'étude de l'encadrement juridique européen et national.
- La lecture transversale se fonde sur une analyse empirique des données recueillies, qui a permis d'identifier les tendances communes et les spécificités nationales. Elle s'illustre notamment par la production de données chiffrées et l'ensemble des tableaux qui accompagnent nos analyses.
- L'étude de terrain, que nous avons brièvement menée auprès des professionnels et acteurs du secteur, a enfin permis de mieux saisir les enjeux et comprendre la technologie.

Conclusions. Si des sensibilités et approches nationales sont observables, nous concluons au terme de notre étude :

- Qu'aucun des États étudiés n'a, à ce jour, adopté de législation spécifique à l'encadrement de la technologie ;
- Que les autorités de protection des données, compétentes, adoptent dans leur majorité une position circonspecte : rappelant les risques liés aux usages de la technologie, elles sont bien souvent les témoins mal armés des expérimentations qui se multiplient ;
- Que les débats nationaux et institutionnels laissent entrevoir l'insuffisance des garanties démocratiques que le législateur est invité à pallier.

Plan du rapport. Le présent rapport est articulé en trois parties : l'identification de l'encadrement européen (I) est suivie d'une cartographie européenne des législations et des usages nationaux (II). La dernière partie étudie la situation propre à chaque État (III).

11 COM(2020) 65 final, Commission européenne, *Intelligence artificielle - Une approche européenne axée sur l'excellence et la confiance*, 19.2.2020, https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_fr.pdf

12 Qui proscrit le recours **à la technologie dans les caméras** corporelles des forces de l'ordre pour trois ans.

PARTIE I.
L'ENCADREMENT EUROPÉEN

Si le débat sur la technologie de reconnaissance faciale a investi la scène européenne, suscitant, force est de constater que la technologie ne fait pas encore l'objet d'un encadrement idoine. Le droit européen n'en est pas pour autant silencieux. Bien que parcellaire, la législation relative à la protection des données à caractère personnel établit un encadrement des usages posant les premiers jalons de l'encadrement de la technologie elle-même. Ces dispositions reposent sur deux textes, adoptés en avril 2016, qui composent le « **paquet européen** » : le **Règlement (UE) 2016/679, du Parlement et du Conseil, relatif à la protection des données des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données** (« RGPD »)[13] d'une part ; la **Directive 2016/680 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** (dite « Directive Police-Justice »)[14], de l'autre.

En parallèle de ces textes, des dispositions sont applicables à l'usage des images faciales dans le cadre de la sécurité et du contrôle aux frontières. Les dispositifs de reconnaissance faciale sont ainsi strictement encadrés en la matière par le **Règlement (UE) 2017/2226[15] du Parlement Européen et du Conseil du 30 novembre 2017 portant création d'un système d'entrée/de sortie (EES) pour enregistrer les données relatives aux entrées, aux sorties et aux refus d'entrée concernant les ressortissants de pays tiers qui franchissent les frontières extérieures des États membres et portant détermination des conditions d'accès à l'EES à des fins répressives, et modifiant la convention d'application de l'accord de Schengen et les règlements (CE) n° 767/2008 et (UE) n° 1077/2011** et par **la réglementation dite « SIS II » relative au système d'information Schengen de deuxième génération composée des règlements 2018/1860[16], 2018/1861[17] et 2018/1862[18].**

Le présent rapport intéresse le recours à la reconnaissance faciale dans la surveillance de l'espace public. Nous préciserons le champ d'application respectif de ces textes (**I**), les régimes établis par ceux-ci quant au traitement des données à caractère personnel sensibles (**II**) puis les dispositions prévoyant l'encadrement des décisions fondées exclusivement sur un traitement automatisé (**III**). Enfin, au regard de la multiplication des initiatives en la matière, les différentes dispositions relatives à l'utilisation des images faciales en matière d'identification biométrique dans le cadre de la sécurité et du contrôle aux frontières seront évoquées à titre accessoire (**IV**).

---

13 Ce texte adopté le 27 avril 2016 remplace l'ancienne directive 95/46/CE du Parlement Européen et du Conseil, du 24 octobre 1995.

14 La directive de 2016 abroge la décision cadre 2008/977/JAI du Conseil.

15 Règlement (UE) 2017/2226 du Parlement Européen et du Conseil du 30 novembre 2017, https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32017R2226&from=EN

16 Règlement (UE) 2018/1860 du Parlement européen et du Conseil du 28 novembre 2018 relatif à l'utilisation du système d'information Schengen aux fins du retour des ressortissants de pays tiers en séjour irrégulier (JO L 312 du 7.12.2018, p. 1-13), https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex:32018R1860

17 Règlement (UE) 2018/1861 du Parlement européen et du Conseil du 28 novembre 2018 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine des vérifications aux frontières, modifiant la convention d'application de l'accord de Schengen et modifiant et abrogeant le règlement (CE) no 1987/2006 (JO L 312 du 7.12.2018, p. 14-55), https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex:32018R1861

18 Règlement (UE) 2018/1862 du Parlement européen et du Conseil du 28 novembre 2018 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine de la coopération policière et de la coopération judiciaire en matière pénale, modifiant et abrogeant la décision 2007/533/JAI du Conseil, et abrogeant le règlement (CE) no 1986/2006 du Parlement européen et du Conseil et la décision 2010/261/UE de la Commission (JO L 312 du 7.12.2018, p. 56-106), https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex:32018R1862

I. Champ d'application du « Paquet Européen »

La Directive Police-Justice, qui définit le régime de traitement des données exploitées à des fins de sûreté, apparaît *prima facie* comme le texte de référence pour la mise en œuvre de la reconnaissance faciale à des fins de surveillance dans l'espace public (**A**). La polysémie des usages mobilise parallèlement le RGPD, contraignant à l'analyse de ses champs d'application territorial et matériel (**B**).

A - Champ d'application matériel de la Directive Police Justice

L'article premier paragraphe 1 de la Directive « Police-Justice » 2016/680 du 27 avril 2016 établit le régime de protection des données personnelles traitées 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 les menaces pour la sécurité publique et la prévention de telles menaces. » Précisons que ce régime concerne exclusivement le traitement de données personnelles par les autorités compétentes - à savoir : les juridictions pénales ou tout autre délégataire de prérogatives de police – et qu'il vise, uniquement le traitement des données à caractère personnel des personnes physiques.

Le cadre législatif européen distingue les traitements de données biométriques en fonction de leur finalité. La reconnaissance faciale constitue un exemple de traitement de données biométriques pouvant être utilisé à diverses fins, allant de la surveillance de l'espace public, aux usages privés « récréatifs » en passant par les usages commerciaux.

En tout état de cause, les usages de la technologie en matière pénale relèvent impérativement de la présente directive.

B - Champ d'application matériel et territorial du RGPD

Le RGPD encadre les activités de traitement des données à caractère personnel, que celles-ci soient automatisées ou non[19]. Ce texte européen ne s'applique qu'à l'égard des données à caractère personnel concernant des personnes physiques[20] vivantes [21]. Les données des personnes morales sont exclues du champ matériel du Règlement[22]. Les dispositions du texte visent tous les supports (papiers et numériques) contenant des données personnelles, ainsi que l'ensemble des responsables de traitements ou sous-traitants.

Les dispositions de **l'article 2 paragraphe 2** précisent les cas où le traitement de données à caractère personnel échappe aux dispositions du RGPD. Sont ainsi concernées :

- les activités ne relevant pas du droit de l'Union européenne ;
- les activités relevant du champ d'application du Chapitre 2 du Titre V du Traité sur L'Union européenne ;
- les activités n'ayant qu'un usage personnel ou domestique ;
- les activités relavant de la directive 2016/680 du 27 avril 2016;

En matière territoriale, l'**article 3 paragraphe 1** du RGPD prévoit son application aux activités des responsables de traitement ou de sous-traitants au sein de l'Union européenne, que ce traitement de données personnelles ait lieu ou non au sein de l'Union. Ainsi, l'**article 3 paragraphe 2** conditionne l'applicabilité du texte par la prise

19 Article 2 §1 « Le présent règlement s'applique au traitement à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier »

20 Considérant 2

21 Considérant 27

22 Considérant 14

en compte du critère d'établissement[23] ou de ciblage[24]. Ces dispositions précitées font peser sur les industriels l'obligation d'assurer la conformité de leurs dispositifs aux exigences européennes en matière de protection des données personnelles.

II. L'encadrement du traitement des données à caractère personnel sensibles

Tout dispositif de reconnaissance faciale repose sur l'exploitation de données biométriques. Ces données relèvent de la catégorie des données dites « sensibles », définies par l'**article 9 du RGPD** comme étant les données « qui révèle(nt) l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits ». Les traitements de ce type de données peuvent constituer un risque d'atteinte aux droits et libertés. La reconnaissance faciale en constitue un exemple typique. Le droit à la vie privé tel que défini à l'article 8 de la Charte des droits fondamentaux de l'Union Européenne est l'un des fondements principaux d'une grande partie des recours contentieux à l'échelle européenne.

Si le paquet européen prohibe leur traitement, celui-ci peut être admis à titre exceptionnel sous certaines conditions (**A**) ; les textes prévoient en outre des dispositions particulières concernant leur encadrement (**B**).

A - La prohibition relative des traitements de données biométriques

Le RGPD interdit le traitement de **données biométriques**[25] définies comme étant des « données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques ». L'article 9 paragraphe 2 prévoit une série d'exceptions. Parmi elles, sont énoncés le consentement libre et éclairé des personnes concernées par le traitement, la sauvegarde des intérêts vitaux de la personne ou l'existence d'un motif d'intérêt public important.

Les lignes directrices européennes[26] prennent l'exemple d'une société privée qui déploie des dispositifs de reconnaissance faciale aux points d'identification dans un aéroport pour vérifier l'identité des passagers. Ceux-ci auraient préalablement consentis à une telle procédure. Les passagers s'inscriront, par exemple, dans un terminal automatique pour créer et d'enregistrer leur gabarit[27] associé à leur carte d'embarquement et à leur identité. Ces lignes directrices rappellent que les points de contrôle avec reconnaissance faciale doivent être clairement distingués de ceux qui en sont dépourvus. Seuls les passagers, ayant préalablement consenti (1) et procédé à leur enregistrement (2), pourront utiliser le portique équipé du système biométrique.

De nouveau, la Directive Police-Justice est plus restrictive quant au traitement de données sensibles. L'article 10 autorise le traitement de ces données « uniquement en cas de nécessité absolue », c'est-à-dire, dans les seuls cas où les traitements:

---

23 Lieu d'établissement du responsable du traitement ou de son sous-traitant.

24 Personnes visées par le traitement.

25 Article 4 du RGPD

26 European Data Protection Board, « Guidelines 3/2019 on processing of personal data through videos devices », January 29, 2019, p.19

27 C'est-à-dire le « modèle facial »

- sont autorisés par le droit de l'Union européenne ou celui d'un État membre ;
- sont destinés à protéger les intérêts vitaux de la personne concernée ou d'une autre personne physique ;
- portent sur des données ayant été manifestement rendues publiques par la personne concernée.

Si la prohibition des traitements de données sensibles est le principe, les exceptions prévues par les textes sont nombreuses. Il apparaît que le régime d'exploitation de ces données est suffisamment large pour autoriser le développement de la reconnaissance faciale au sein de l'UE.

B - Les mesures d'encadrement des traitements de données biométriques

L'entrée en vigueur du paquet européen renverse le paradigme en substituant une démarche de conformité à l'obtention d'une autorisation préalable de l'autorité de régulation pour la mise en place d'un traitement. En matière de reconnaissance faciale cet inversement de logique entraîne des conséquences importantes pour les responsables de traitements, qui doivent en garantir la conformité. Dans cette perspective, deux mécanismes prévus par la réglementation européenne conditionnent le déploiement des dispositifs. C'est en premier lieu, la réalisation d'une analyse d'impact relative à la protection des données[28] (AIPD) (**1**) et en second, l'intégration dès la conception (*privacy by design*) et par défaut de la vie privée (*privacy by default*) qui en découle (**2**). En cas de non-respect de ces obligations, les responsables de traitement prennent le risque d'être sanctionnés.

1. L'analyse d'impact relative à la protection des données

Les textes européens convergent quant à la détermination des traitements qui doivent faire l'objet d'une AIPD. **L'article 35 du RGPD et l'article 27 de la Directive Police-Justice** imposent aux responsables de traitement de réaliser **une analyse d'impact** en cas de « risque élevé pour les droits et libertés des personnes physiques ». Ce risque existe dès lors que des données biométriques sont traitées à des fins d'identification ou d'authentification d'une personne de manière unique[29].

A l'issue de cette AIPD, les **articles 36 du RGPD et 28 (a) de la Directive Police-Justice** exigent en outre que le responsable de traitement consulte l'autorité de contrôle lorsqu'une analyse d'impact relative à la protection des données « indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque ».

Enfin, contrairement à l'**article 35** du RGPD qui identifie les traitements particuliers devant faire l'objet d'une AIPD[30], la Directive Police-Justice demeure muette sur le sujet. Toutefois, les différentes autorités de régulations des Etats membres ont établis des listes de traitements soumis obligatoirement à une AIPD et le CEPD a fixé une liste de neuf critères[31] pour déterminer si une analyse d'impact est nécessaire. Si un traitement répond à au moins deux critères celui-ci doit faire l'objet d'une AIPD.

---

28 La CNIL précise à ce titre que « tout projet d'y recourir devra à tout le moins faire l'objet d'une analyse d'impact relative à la protection des données (AIPD) » https://www.cnil.fr/fr/definition/reconnaissance-faciale

29 Voir Considérant n°51 de la Directive Police-Justice et l'article 35 paragraphe 3, b) du RGPD

30 « a) l'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire;
b) le traitement à grande échelle de catégories particulières de données visées à l'article 9, paragraphe 1, ou de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10; ou
c) la surveillance systématique à grande échelle d'une zone accessible au public. »

31 Groupe de travail « Article 29 », Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du règlement (UE) 2016/679 adoptées le 4 avril 2017 - Version révisée et adoptée le 4 octobre 2017 (WP248rev.01), p.27 https://www.cnil.fr/sites/default/files/atoms/files/wp248_rev.01_fr.pdf

Dans le cadre des usages de la reconnaissance faciale, qui conduisent, dans la majorité des cas, à effectuer une surveillance à grande échelle d'un espace public, le traitement fait obligatoirement l'objet d'une AIPD préalable et ce, indépendamment du cadre dans lequel elle est déployée. Comme évoqué dans les développements précédents, cette exigence est aussi bien consacrée par le RGPD que par la directive Police-Justice.

2. La protection des données dès la conception (by design) et par défaut (by default)

Le CEPD a publié en novembre 2019 ses lignes directrices[32] relatives aux concepts de *privacy by design* et *by default* pour en préciser les contours. Ces concepts, tels que définis par le RGPD[33], apparaissent comme des principes d'encadrement des traitements de données personnelles.

- ⇨ Le concept **de *privacy by design*** implique de prendre en compte la protection des données personnelles dès la conception du produit ou du service reposant sur un traitement de donnée. Concrètement, sont implémentés dans le dispositif technique des systèmes permettant d'assurer la protection des données, comme le chiffrement des données, leur pseudonymisation ou encore leur minimisation. L'adoption de mesure techniques et organisationnelles pèse sur le responsable de traitement et assure sa conformité au RGPD.
- ⇨ Le principe de ***privacy by default***[34] enjoint les responsables de traitement d'assurer que leur produit ou service réponde, par défaut[35], au plus haut niveau de protection.

Ces concepts impliquent donc que la règle de droit soit mise en œuvre par le biais de l'architecture du dispositif. En matière de reconnaissance faciale, ils peuvent par exemple se traduire par les mesures telles que le floutage des visages, la présence de caches devant les lieux d'habitation, l'absence d'enregistrement des images faciales des personnes non recherchées ou le hachage des gabarits. Face aux controverses entourant l'effectivité de la procédure d'AIPD, ces principes s apparaissent comme des mesures décisives d'encadrement de la technologie.

Conformément à l'**article 42 du RGPD**, ces mesures peuvent donner lieu à une certification des dispositifs.

III. L'encadrement des décisions fondées exclusivement sur un traitement automatisé

Le RGPD et la Directive Police-Justice interdisent la prise de décision individuelle sur le fondement exclusif d'un traitement automatisé. Des dérogations à cette prohibition sont prévues, mais elles diffèrent selon les textes.

L'**article 22 paragraphe 2 du RGPD** envisage trois **exceptions** :

- En cas de nécessité à la conclusion ou à l'exécution d'un **contrat** entre la personne concernée et un responsable du traitement ;
- En cas **d'autorisation** par le droit de l'Union européenne ou par le droit de l'État membre auquel le responsable du traitement est soumis ;
- En cas de **consentement** explicite de la personne concernée.

32 European Data Protection Board, « Guidelines 4/2019 on Article 25 Data Protection by Design and by Default », Novembre 29, 2019, p.27 https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf

33 Article 25 paragraphe 1 du RGPD

34 Article 25 paragraphe 2 du RGPD

35 Sans configuration externe

Lorsqu'une décision est prise sur le fondement d'un traitement automatisé, des *« mesures appropriées pour la sauvegarde des droits et libertés et des* intérêts *légitimes de la personne concernée »* doivent être mises en œuvre. **L'article 22 du RGPD** impose une « intervention humaine »[36], sauf lorsque la décision repose sur le consentement explicite de la personne concernée ou lorsqu'elle est nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et un responsable de traitement. Dès lors, et conformément au **considérant n°71**, toute personne concernée réceptrice d'une décision individuelle automatisée est en *« droit d'obtenir une* intervention humaine, d'exprimer son point de vue, d'obtenir une explication quant à la d*écision prise à l'issue de ce type d'évaluation et de contester la dé*cision ».

Ce même considérant précise en outre qu'un enfant ne devrait pas faire l'objet d'une décision prise sur le fondement d'un traitement automatisé. Les lignes directrices du G29 relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679 estiment toutefois « qu'il ne s'agit pas d'une interdiction absolue de ce type de traitement à l'égard des enfants » bien qu'il « recommande aux responsables de traitement de ne pas invoquer, en principe, les exceptions prévues à l'**article 22 paragraphe 2** pour le justifier ».[37] Les garanties mises en place doivent être adaptées aux enfants. La nécessité d'une protection spécifique pour ces derniers est affirmée au **considérant n°3**[38]. Ces dispositions prennent tout leur sens au regard des différentes expérimentations, abouties ou non, au sein des établissements publics scolaires, notamment en France et en Suède.

La directive Police-Justice est plus restrictive : elle n'admet qu'une seule exception à l'interdiction suscitée. L'**article 11** subordonne le traitement à « l'autorisation par le droit de l'Union européenne ou par le droit de l'État membre auquel le responsable de traitement est soumis ». Le consentement de la personne concernée ne peut constituer une exception justifiant la prise d'une décision individuelle automatisée[39]. **Le considérant n°35** soutient en effet que *« lorsqu'elle est tenue de respecter une obligation légale, la personne concernée ne dispose pas d'une véritable liberté de choix ; sa réaction ne pourrait dès lors être considérée comme une manifestation libre de sa volonté ».*

Lorsqu'un traitement est mis en œuvre, **l'article 11 de la directive** octroie à la personne concernée *« le droit d'obtenir une intervention humaine de la part du responsable du traitement ».* **Le considérant n°38** est plus explicite en précisant que la personne concernée reçoit des informations spécifiques et dispose du droit *« d'exprimer son point de vue, d'obtenir une explication quant à la décision prise à l'issue de ce type d'évaluation ou de contester la décision ».* En outre, la directive interdit expressément *« tout profilage qui entraîne une discrimination à l'égard des personnes* physiques sur la base des catégories particulières de données à caractère personnel visées à l'article 10 ».

Au regard de l'ensemble de ces développements, il apparaît que les dispositions européennes encadrent largement l'utilisation des nouvelles technologies reposant sur le traitement automatique de données à caractère personnelle. Toutefois aucune n'est spécifique à la reconnaissance faciale. Les textes sont parfois trop éloignés des véritables risques que présentent les usages. Ce constat encourage plusieurs certaines autorités nationales de contrôle à plaider en faveur de l'instauration d'un cadre juridique spécifique à la technologie.

---

36 De la part du responsable de traitement

37 Groupe de travail « Article 29 », Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679 adoptées le 3 octobre 2017 - Version révisée et adoptée le 6 février 2018 (WP251rev.01), p.32

38 *Ibid.*

39 Groupe de travail « Article 29 », Lignes directrices relatives au consentement aux fins du règlement (UE) 2016/679 adoptées le 28 novembre 2017 - Version révisée et adoptée le 10 avril 2018 (WP259rev.01), p.36

IV. Les dispositions relatives à l'usage des images faciales comme éléments d'identification biométriques

Différents textes européens prévoient parallèlement des dispositions spécifiques à l'utilisation de la reconnaissance faciale aux fins d'identification, notamment en matière de sécurité et de contrôle aux frontières.

Le Règlement *Entry – Exit System* (EES) du 30 novembre 2017 relatif à la création d'un système d'entrée et de sortie à conduit à généraliser l'utilisation des images faciales comme moyens d'identification biométriques dans les différents systèmes informatiques existants au sein de l'Union[40]. Ce texte ouvre véritablement la voie au développement des dispositifs de reconnaissance faciales en généralisant l'usage des images faciales pour la vérification d'identité, les demandes de visa, d'asile et plus largement le passage aux frontières. Interconnectées avec d'autres données, les données biométriques ont pour finalités d'améliorer l'efficacité des contrôles. Le **considérant n°20** du Règlement précise que « [l]'utilisation de l'image faciale en combinaison avec les données dactyloscopiques permet de réduire le nombre total d'empreintes digitales dont l'enregistrement est requis tout en garantissant le même résultat quant à la précision de l'identification ».

Le Règlement du 28 décembre 2018 sur l'utilisation du *Schengen Information System* pour la vérification aux frontières prévoit des dispositions spécifiques quant aux conditions de collectes des images faciales, l'utilisation des dispositifs de reconnaissance faciale et les droits des personnes concernées par le traitement. Son **considérant n°22** précise que « [l]e présent règlement devrait définir les conditions d'utilisation des données dactyloscopiques, des photographies et des images faciales à des fins d'identification et de vérification. Les images faciales et les photographies ne devraient être utilisées, dans un premier temps, à des fins d'identification que dans le contexte des points de passage frontalier habituels. Une telle utilisation devrait faire l'objet d'un rapport de la Commission confirmant que la technique requise est disponible, fiable et prête à être employée. ».

Enfin, le recours à la reconnaissance faciale dans le contrôle aux frontières est également évoqué dans les débats relatifs à l'extension du traité de Prüm. Ce traité, institué en 2008 par la Décision 2008/615/JAI du Conseil du 23 juin 2008 relative à l'approfondissement de la coopération transfrontalière, vise notamment à lutter contre le terrorisme et la criminalité transfrontalière[41]. Il facilite à cet effet les échanges automatisés de données (ADN, dactyloscopiques, d'immatriculations) entre les Etats parties. Les travaux en cours au sein de la Commission Européenne pourraient conduire à accroître l'assiette des données biométriques partagées et l'interconnexion des bases de données de reconnaissance faciale de la police des vingt-sept Etats membres de l'Union Européenne.[42].

---

40 FRA, « Facial recognition technology : fundamental rights considerations in the context of law enforcement », Table 2 : EU IT systems for migration and security and processinf of facial images, p.14 https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf

41 **Décision 2008/615/JAI du Conseil du 23 juin 2008 relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière,** https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex:32008D0615. Cette décision est issue de la signature d'un traité en 2005 par sept Etats membre de l'Union Européenne parmi lesquels la France, la Belgique, l'Espagne, l'Allemagne, les Pays Bas, le Luxembourg et l'Autriche

42 Z. Campbell, C. Jones, « Leaked reports show EU police are planning a pan-européan network of facial recognition databases » [en ligne], *The Intercept*, February 21, 2020, [consulté en ligne le 18/03/2020], https://theintercept.com/2020/02/21/eu-facial-recognition-database/

PARTIE II.
CARTOGRAPHIE EUROPÉENNE DES LÉGISLATIONS ET DES USAGES NATIONAUX

Dans chacun des pays étudiés – l'Allemagne, la Belgique, l'Espagne, la France, l'Italie, les Pays Bas, la République tchèque, le Royaume-Uni et la Suède - la présente étude interroge la législation nationale en vigueur (I), la position des autorités de protection des données nationale (II) et les expérimentations conduites dans l'espace public (III). Une dernière section est consacrée aux résistances et recours introduits à l'encontre des dispositifs de reconnaissance faciale (IV.)

I. Législation

Le pays concerné dispose-t-il d'une législation spécifique à la reconnaissance faciale ou, du moins, de dispositions autorisant son déploiement ?

A ce jour aucun État européen, parmi ceux étudiés, n'ont adopté de dispositions spéciales visant à encadrer les usages de la technologie (A). Si la nécessité de réaliser une étude d'impact préalablement à son déploiement est établie, le bilan de ces études est mitigée faute de publicité obligatoire (B). Des dispositions spécifiques aux mineurs ont été rappelées dans certains Etats (C).

A - Absence de législation spéciale

A ce jour, aucun État européen - parmi ceux étudiés - n'a adopté un encadrement légal spécifique à la reconnaissance faciale. Les expérimentations réalisées sont principalement régies par le droit européen de la protection des données et ses retranscriptions nationales. Ces dispositions sont complétées, dans certains Etats :

- Par la législation relative à la vidéoprotection ; tel est le cas de la Belgique[43], la France[44] et du Royaume-Uni[45].
- Par les dispositions spécifiques au traitement des données par les autorités de police en Suède[46].

Les usages de la technologie n'en alimentent pas moins le débat public et les propositions d'encadrement se multiplient. Celles-ci traduisent une préférence pour l'approche sectorielle : les propositions visent principalement à encadrer le recours à la reconnaissance faciale par les forces de police d'une part, dans les stades de l'autre.

- **Perspectives d'encadrement des usages de la reconnaissance faciale par les forces de police**

Deux initiatives peuvent être mentionnées à ce titre:

- Plusieurs propositions de loi ont été déposées en France[47], pour répondre à la volonté forte de certains élus d'adopter la technologie et équiper les forces de police.

43 Loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2007032139&table_name=loi

44 Code de la sécurité intérieure (CSI) : Article L251-1 à L255-1 ainsi que les articles L223-1 à L223-9 en matière de lutte contre le terrorisme et les atteintes aux intérêts fondamentaux de la nation.

45 *Surveillance Camera Code of Practice*, Juin 2013, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/282774/SurveillanceCameraCodePractice.pdf

46 Lag (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område, https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-20181693-om-polisens-behandling-av_sfs-2018-1693

47 Par exemple, la proposition de loi relative à la reconnaissance faciale dans les enquêtes terroristes et la prévention des attentats, déposée par la Députée Marine Brenier en septembre 2017.

- Au Royaume-Uni, l'*Information Commissioner's Office* plaide pour l'adoption d'un code de pratique juridiquement contraignant à destination des forces de police[48].

▪ **Perspectives d'encadrement des usages dans les stades**

Deux propositions ont été recensées :

- La République Tchèque envisage d'encadrer plus spécifiquement les usages de la technologies pour limiter l'accès aux stades à certains individus identifiés[49].
- En France, d'après les entretiens que nous avons réalisés[50], une loi d'expérimentation serait envisagée pour permettre l'utilisation des dispositifs de reconnaissance faciale dans le cadre de l'organisation des Jeux olympiques de 2024.

Notons que ces propositions font écho aux expériences, nombreuses, conduites dans les stades. Cinq Etats[51] parmi les douze étudiés ont vu la mise en œuvre d'expérimentations visant à contrôler les accès.

B - Analyse d'impact : bilan en demi-teinte

Nous constatons qu'aucun des Etats étudiés n'a pris de mesures particulières visant à renforcer les dispositions relatives aux analyses d'impact prévues par les textes européens[52].

Plusieurs autorités de protection ont toutefois rappelé la nécessité de conduire celle-ci dans le cadre des usages de la reconnaissance faciale ; tel est le cas des autorités belge[53], espagnole[54], française[55], tchèque et britannique[56]. Deux autorités ont en outre adopté des sanctions en l'absence de sa réalisation :

- L'autorité de protection des données suédoise, qui prononça une sanction à l'encontre d'un établissement public scolaire ayant mis en place un logiciel de reconnaissance faciale[57].
- L'Organe de contrôle de l'information policière belge, qui a temporairement interrompu un projet de reconnaissance faciale au sein de l'aéroport de Bruxelles-National sur ces mêmes motifs[58].

Les informations obtenues ne permettent pas d'avoir une vision exhaustive de l'ensemble des analyses d'impacts effectuées dans le cadre des usages de la technologies[59].

48 Information Commissioner's Opinion, "The use of live facial recognition technology by law enforcement in public places", 31 octobre 2019, p. 3, https://ico.org.uk/media/about-the-ico/documents/2616185/live-frt-law-enforcement-report-20191031.pdf

49 CT24, « Poznala vás kamera, na stadion nemůžete. Ministerstvo chystá zákon proti výtržníkům » [en ligne], *CT24*, 16 février 2020, [consulté le 01/02/2020], https://ct24.ceskatelevize.cz/domaci/3048906-poznala-vas-kamera-na-stadion-ne-muzete-ministerstvo-chysta-zakon-proti-vytrznikum

50 Voy. *Infra* (Interviews)

51 Le Danemark, la Belgique, la République tchèque, la France et le Royaume-Uni.

52 Voy. *Infra* (Partie I).

53 Secrétariat Général de l'Autorité de protection des données, « Adoption de la liste des catégories de traitement devant faire l'objet d'une analyse d'impact relative à la protection des données conformément à l'article 35.4 du Règlement Général sur la Protection des données (CO-A-2018-001) », n°01/2019, 16 janvier 2019, https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/01_2019_SG.pdf

54 Agencia Española de Protección de Datos, « Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD », https://www.aepd.es/sites/default/files/2019-09/guia-analisis-de-riesgos-rgpd.pdf

55 Commission Nationale de l'Informatique et des Libertés, « Liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données n'est pas requise », https://www.cnil.fr/sites/default/files/atoms/files/liste-traitements-aipd-non-requise.pdf

56 Information Commissioner's Office, "Examples of processing 'likely to result in high risk' ", https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/examples-of-processing-likely-to-result-in-high-risk/

57 La décision reposait en partie sur l'absence de réalisation d'une AIPD. Datainspektionen, "Tillsyn enligt EU:s dataskyddsförordning 2016/679 – ansiktsigenkänning för närvarokontroll av elever", 20 août 2019, https://www.datainspektionen.se/globalassets/dokument/beslut/beslut-ansiktsigenkanning-for-narvarokontroll-av-elever-dnr-di-2019-2221.pdf

58 B. Schmitz, « Le RWDM comme laboratoire pour une technologie de reconnaissance faciale » [en ligne], RTBF, 5 septembre 2018, [consulté le 14/01/2020], https://www.rtbf.be/info/regions/bruxelles/detail_le-rwdm-comme-laboratoire-pour-une-technologie-de-reconnaissance-faciale?id=10011249

59 Rappelons en effet qu'il n'existe pas d'obligation légale de publication en dépit des recommandations formulées par le Comité Européen de la Protection des Données. CEDP, Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est «susceptible d'engendrer un risque élevé» aux fins du

C - Des dispositions spécifiques relatives aux mineurs

Certains États ont adopté des mises en garde spécifiques aux mineurs ; tel est le cas de l'Allemagne et de l'Espagne.

- ⇨ En Allemagne, la Commission Éthique d'Allemagne souhaite sensibiliser le gouvernement fédéral pour que celui-ci offre des solutions technologiques aux familles. Ces solutions doivent assurer une protection accrue aux mineurs et prévenir le risque de profilage ; ils doivent aussi permettre aux mineurs d'exercer leur droit à l'autodétermination informationnelle dans un environnement numérique sain[60].

- ⇨ En Espagne, la loi organique sur la protection des données à caractère personnel du 5 décembre 2018[61] prévoit des dispositions spécifiques aux mineurs. L'article 7 relatif au consentement des mineurs dispose que le traitement des données à caractère personnel ne peut être fondé sur le consentement d'un mineur de moins de quatorze ans. A défaut de cette majorité numérique, le traitement est soumis au consentement du titulaire de l'autorité parentale ou de la tutelle. Ce titulaire, en représentation du mineur et conformément à l'article 12 de la loi organique, peut également exercer les droits prévus par cette même loi (droit d'accès, de rectification, etc).

  Dans le cadre spécifique du traitement des données à caractère personnel lors de l'utilisation de dispositifs de reconnaissance faciale, l'autorité de contrôle espagnole a publié des lignes directrices[62] dans lesquelles elle rappelle cette obligation.

II. Prise de position des autorités de contrôle

Quelles sont les positions adoptées par les autorités nationales de protection des données si - et dans la positive lorsque - celle-ci se sont prononcées? D'autres autorités nationales ont - elles pris position, de manière concurrente ou complémentaire, sur le sujet ?

En l'absence de cadre juridique idoine, les autorités nationales de protection des données personnelles ont, pour la plupart, été conduites à se prononcer sur les usages de la reconnaissance faciale (A). Parallèlement, d'autres instances nationales, concurrentes ou complémentaires, ont pris position en soutien ou en contradiction des premières, suscitant débats et interrogations (B).

A - Positions des autorités nationales de la protection des données personnelles

Toutes les autorités nationales de protection des données personnelles saisies se sont reconnues compétentes en matière de reconnaissance faciale dans deux hypothèses :

- La formulation d'une recommandation ou d'une décision relative(s), expressément, à la technologie[63] ;
- Une prise de position indirecte en se prononçant plus généralement sur les données biométriques[64].

Au départ de ces différents documents, et des positionnements adoptés, nous distinguons les autorités de contrôle en quatre catégories : les autorités de contrôle réservées **(1)** ; les autorités de contrôle mitigées **(2)** ; les autorités de contrôle défavorables **(3)** ; les autorités de contrôle favorables **(4)**.

1. Les autorités de contrôle réservées

Sont identifiées comme « réservées », les autorités de contrôle qui n'interdisent pas le recours à la technologie, mais en soulignent les **risques**, et appellent à en **limiter les usages** dans le respect des droits et libertés des citoyens.

règlement (UE) 2016/679, https://www.cnil.fr/sites/default/files/atoms/files/wp248_rev.01_fr.pdf

60 Voy. Infra, Allemagne.

61 Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16673

62 Agencia Española de Protección de Datos, « Orientaciones para centros educativos - Informe sobre la utilización por parte de profesores y alumnos de aplicaciones que almacenan datos en nube con sistemas ajenos a las plataformas educativas », 6 mars 2018, https://www.aepd.es/sites/default/files/2019-09/guia-orientaciones-apps-datos-alumnos.pdf

63 C'est le cas des Pays-Bas, de l'Italie, la France, le Royaume-Uni, la Suède, l'Allemagne

64 C'est le cas de la Belgique, l'Espagne, La République Tchèque.

Les autorités de contrôle de la France, l'Espagne, la Belgique et la Suède s'inscrivent dans cette catégorie. Elles formulent en ce sens des recommandations pour son encadrement.

- ⇨ La **CNIL française**, soucieuse des risques technologiques et de leur potentiel liberticide, appelle à la prudence. Elle souligne la nécessité d'une approche casuistique et plaide en faveur d'un « *débat à la hauteur des enjeux* » [65].
- ⇨ L'**autorité de contrôle suédoise** invite son gouvernement à légiférer[66]. Parmi les avis émis[67] elle reconnaît la légalité de certaines expérimentations (usages par les forces de police) et en sanctionne d'autres, à l'instar de celle conduite dans le lycée de la ville de Skellefteå.
- ⇨ L'**Agence espagnole** de protection des données ne s'est pas prononcée sur des cas d'usage. Elle a toutefois adopté une position plus générale, refusant de conférer un blanc-seing aux autorités et rappelant la nécessité d'observer les grands principes applicables en matière de protection des données[68]. Elle dénonce en ce sens l'installation de vidéo surveillance dans le but de contrôler les fréquentations scolaires.
- ⇨ L'**Autorité de protection des données personnelles belge** a formulé un avis relatif à l'usage des données biométriques dans le cadre de l'authentification des personnes. Si elle reconnait la « forte fiabilité » de ses technologies sur le principe, elle émet une réserve importante quant au risque de taux d'erreur. La biométrie ne devrait pas être utilisée, selon elle, au seul motif d'être l'unique moyen pour réaliser le but recherché, ou parce qu'elle est pratique et «fait moderne»[69].

2. Les autorités de contrôle mitigées

Nous attribuons la position « mitigée » aux autorités de contrôle qui adoptent des positions ambiguës. L'ambiguïté procède le plus souvent du décalage entre des prises de position publiques assertives, condamnant l'usage de la technologie de reconnaissance faciale, et des décisions ou avis autorisant très largement expérimentations et usages.

- ⇨ Tel est le cas de **l'autorité de contrôle anglaise**. *L'Information Commissioner's Office* multiplie les déclarations publiques alertant des risques de biais et de discriminations liés aux usages de la reconnaissance faciale[70]. Elle plaide en outre pour l'adoption d'un code de pratiques contraignantes[71]. Dans le même temps, l'autorité de contrôle anglaise ne s'est opposée à aucune expérimentation de la reconnaissance faciale.
- ⇨ Aux Pays-Bas, l'ambiguïté résulte de prises de position contradictoire. En février 2004, **l'autorité de contrôle hollandaise** affirmait que la capture des données biométriques d'une foule aux fins d'identification d'une personne était disproportionnée. Elle autorisait pourtant, en juin 2018, les publicitaires à utiliser la reconnaissance faciale dans l'espace public pour analyser l'humeur, le sexe et l'âge des passants afin de leur proposer des publicités adéquates[72].

3. Les autorités de contrôle défavorables

65 *Voy. infra (France)*

66 *Voy. infra (Suède)*

67 Datainspektionen, « Polisen får använda ansiktsigenkänning för att utreda brott », 24 octobre 2019, https://www.datainspektionen.se/nyheter/polisen-far-anvanda-ansiktsigenkanning-for-att-utreda-brott/ ; Datainspektionen, « Lagändring krävs för att polisen ska kunna utföra testverksamhet av ansiktsverifiering på flygplats », 16 décembre 2019, https://www.datainspektionen.se/nyheter/lagandring-kravs-for-att-polisen-ska-kunna-utfora-testverksamhet-av-ansiktsverifiering-pa-flygplats/

68 *voy. infra (Espagne)*

69 Voy. *infra (Belgique),* Autorité de la protection des données, « Un choix de société », https://www.autoriteprotectiondonnees.be/un-choix-de-soci%C3%A9t%C3%A9

70 Information Commissioner's Office, "Human bias and discrimination in AI systems", 25 juin 2019, https://ico.org.uk/about-the-ico/news-and-events/ai-blog-human-bias-and-discrimination-in-ai-systems/

71 Voy. *infra* (Royaume-Uni).

72 Voy. *infra* (Pays-Bas).

Sont « défavorables », les autorités de contrôles qui refusent la mise en place de ces dispositifs. Parmi les Etats étudiés, seule **l'autorité de contrôle allemande** est assimilable à une telle position. Selon elle, la technologie ne peut légalement être déployée en l'absence de base légale, laquelle fait aujourd'hui défaut[73]. Pour le commissaire fédéral à la protection des données, l'absence de fiabilité est préjudiciable et liberticide : « les gens sont suspectés à tort. Nous menaçons de perdre l'équilibre entre sécurité et liberté.[74] ».

4. Les autorités de contrôle favorables

Sont « favorables » aux usages de la reconnaissance faciale, les autorités de contrôle qui approuvent, sans nuance, les expérimentations conduites. Seule l'Italie, parmi les Etats étudiés, incarne cette position.

- ⇨ **L'autorité de contrôle italienne** a approuvé la majorité des expérimentations initiées75. L'autorité juge le traitement de données biométriques conforme aux exigences de l'article 7 du décret législatif du 18 mai 2018, qui exige la stricte nécessité du traitement ainsi que des garanties adéquates pour les droits et libertés76. Par ailleurs, elle estime que ce traitement de données sensibles ne tombe pas sous le coup de l'interdiction des décisions fondées uniquement sur un traitement automatisé prévue à l'article 8 du décret législatif du 18 mai 201877. Enfin, un tel traitement serait compatible avec le principe de minimisation des données78 en ce sens que la biométrie faciale peut - dans le cas de la gestion des flux - éviter le recoupement de plusieurs données d'identification.

B - Positions des instances concurrentes ou complémentaires

Outre les autorités de contrôle officielles assurant le respect du droit au traitement des données personnelles, d'autres instances sont amenées à s'exprimer sur la légalité des usages de la reconnaissance faciale lorsqu'ils concernent le maintien de l'ordre public. Parmi elles :

- ⇨ L'**Organe de contrôle de l'information policière belge**. Cet organe est une institution parlementaire fédérale autonome, disposant de la compétence exclusive en matière de protection des données personnelles pour les traitements réalisés par la police.
- ⇨ Le **Royaume-Uni** dispose également de plusieurs **autorités de contrôle**[79] et d'un **comité parlementaire** afin d'épauler l'autorité britannique de protection des données[80]. Elles sont amenées à prendre position[81] et émettre des conseils afin d'encadrer les usages de la reconnaissance faciale. Quatre instances distinctes se sont prononcées sur le déploiement de la technologie.
- ⇨ En **Allemagne**, la **Commission d'éthique fédérale sur les données**[82] a été mise en place par le gouvernement fédéral. Elle apporte son expertise légale et technique au gouvernement et au Parlement au travers de recommandations écrites[83]. Elle bénéficie d'un rôle consultatif sur les questions relatives aux algorithmes et à l'intelligence artificielle, mais le Commissaire à la protection des données dispose, seul, d'un rôle décisionnel.

73 Voy. *infra* (Allemagne).

74 *« Menschen geraten zu Unrecht unter Verdacht. Wir drohen die Balance zwischen Sicherheit und Freiheit zu verlieren".* Ulrich kelber, « *Le responsable de la protection des données met en garde contre la reconnaissance automatique des visages* » [en ligne], *t3n*, 16 janvier 2019, [consulté le 16/01/2020]. https://t3n.de/news/datenschutzbeauftragter-kelber-1137512/ Traduction par nous.

75 Voy. *infra* (Italie)

76 Garante Per La Protezione Dei Dati Personali, **Décision n°9040256 rendue le 26 juillet 2018.**

77 *Ibidem.*

78 Garante Per La Protezione Dei Dati Personali, **Décision n°**8789277 rendue le 15 mars 2018.

79 Le Surveillance Camera Commissionner, le Biometrics Commissionner et le Science and Technology Committee.

80 Information Commissionner's Office

81 Biometrics Commissioner, "Response to announcement on Live Facial Recognition", 24 janvier 2020, https://www.gov.uk/government/news/response-to-announcement-on-live-facial-recognition

82 "*Daten Ethik Kommission*"

83 Site officiel de la Commission d'éthique fédérales sur les données https://datenethikkommission.de

⇨ En **France**, l'avis de la **Commission départementale de la vidéoprotection** est requis pour la délivrance des autorisations permettant d'installer des caméras de vidéoprotection[84]. Son intervention est toutefois limitée car dès lors qu'un traitement automatisé des données est mis en place, c'est la CNIL qui intervient[85]. La CNIL demeure prépondérante sur les questions de reconnaissance faciale.

Les positions peuvent se révéler divergentes **(1)**, concordantes **(2)** ou complémentaires **(3)**.

1. Divergence

⇨ Au **Royaume-Uni**, le *Science and Technology Committee* s'est positionné sur la reconnaissance faciale avec beaucoup plus de fermeté que l'*Information Commissionner's Office* (ICO). Le comité parlementaire relevant de la Chambre des communes estime que cette technologie ne devrait pas être déployée tant que son efficacité et les risques de biais n'auront pas été élucidés. Il se positionne donc en faveur d'une interdiction de toute autre expérimentation tant qu'un cadre législatif n'aura pas été mis en place[86]. L'ICO, au contraire, fait preuve de plus de pragmatisme : si elle soutient fortement l'adoption d'un code de bonnes pratiques contraignant pour encadrer les usages de la reconnaissance faciale[87], elle ne s'oppose pas à l'expérimentation de la technologie mais incite les acteurs à coopérer avec elle.

2. Concordance

⇨ La **Commission d'éthique fédérale allemande** sur les données[88] identifie la reconnaissance faciale comme présentant un danger pour la vie privée et la préservation des libertés fondamentales. Elle s'inscrit en ce sens dans la lignée des recommandations formulées par le Commissaire fédéral à la protection des données, en identifiant des problématiques qui n'avaient jusqu'à lors pas été mentionnées par l'autorité de contrôle. Elle mentionne notamment le risque de développement de réseaux informationnels non officiels entre les instances gouvernementales qui s'en trouverait facilité par la collecte des données à grande échelle ; et par là même, un risque de profilage des individus. Elle invite à ce titre le gouvernement fédéral à renforcer les obligations de transparence voire à créer des dispositions juridiques spécifiques encadrant l'exploitation de ces données biométriques[89].

⇨ **Au Royaume-Uni**, les positions du *Surveillance Camera Commissioner* et du *Biometrics Commissioner* convergent vers le même positionnement que celui de l'autorité de protection des données. Chacune de ces deux instances a tenu à s'exprimer suite au jugement *R. (Bridges) c. SWP & SSHD*[90] rendu par la *High court* de Cardiff sur l'utilisation de la technologie de reconnaissance faciale en direct par la police de Cardiff. Dans une position convergente avec l'opinion de l'ICO publiée le 31 octobre 2019[91],

---

84 Article L252-1 alinéa 1 du Code de la Sécurité Intérieure

85 Article L252-1 alinéa 2 du Code de la Sécurité Intérieure : « utilisés sur la voie publique ou dans des lieux ouverts au public dont les enregistrements sont utilisés dans des traitements automatisés ou contenus dans des fichiers structurés selon des critères permettant d'identifier, directement ou indirectement, des personnes physiques »

86 Science and Technology Committee, "The work of the Biometrics Commissioner and the Forensic Science Regulator" 17 juillet 2019, https://publications.parliament.uk/pa/cm201719/cmselect/cmsctech/1970/1970.pdf

87 Information Commissioner's Opinion, "The use of live facial recognition technology by law enforcement in public places" 31 octobre 2019, p. 3, https://ico.org.uk/media/about-the-ico/documents/2616185/live-frt-law-enforcement-report-20191031.pdf

88 "Data Ethik Kommission"

89 « The Data Ethics Commission believes that there is particular potential for abuse if individual subsystems are connected, resulting in the pooling of data and analytical findings from very different areas and sectors, which significantly steps up the intensity of surveillance [...] clear legal limits [...] must be imposed on the exchange of information and patterns between authorities » §3.2.3 p.102 https://www.bmjv.de/SharedDocs/Downloads/DE/Themen/Fokusthemen/Gutachten_DEK_EN_lang.pdf?__blob=publicationFile&v=3

90 High Court of Justice, Cardiff, *R (Bridges) v. CCSWP and SSHD*, [2019] EWHC 2341 (ADMIN), § 137, https://www.judiciary.uk/wp-content/uploads/2019/09/bridges-swp-judgment-Final03-09-19-1.pdf

91 Information Commissioner's Opinion, "The use of live facial recognition technology by law enforcement in public places", 31 octobre 2019, p. 3, https://ico.org.uk/media/about-the-ico/documents/2616185/live-frt-law-enforcement-report-20191031.pdf

le *Surveillance Camera Commissioner*[92] et le *Biometrics Commissioner*[93] ont tous deux souligné que ce jugement d'espèce ne devait pas être interprété comme une autorisation générale d'utiliser la reconnaissance faciale pour les forces de police. Toutes deux manifestent également leur intérêt en faveur de l'adoption d'un cadre juridique pour une bonne gouvernance des utilisations futures de cette technologie.

3. Complémentarité

⇨ Les positions divergent parfois de celles des autorités de contrôle des données. Tel fut le cas de l'**Organe de contrôle de l'information policière belge**. Cet organe est une institution parlementaire fédérale autonome, disposant de la compétence exclusive en matière de protection des données personnelles pour les traitements réalisés par la police. Il fut appelé à se prononcer sur la mise en place de la reconnaissance faciale par la police au sein de l'aéroport Bruxelles-National[94]. Contrairement à l'Autorité de protection des données personnelles, son avis est expressément défavorable : si le recours à la vidéosurveillance est légal sur le territoire, tel n'est pas le cas pour la reconnaissance faciale, dispositif plus intrusif pour les droits et libertés des personnes.

III. Cas d'usage

Quelle(s) expérimentation(s) de la technologie ont été conduite dans l'espace public de chacun des Etats ? Quelles en ont été les conditions et les conclusions ?

En Europe, la technologie de reconnaissance faciale a fait l'objet de diverses expérimentations dans l'espace public **(A)**. Parmi elles, nombreuses procèdent d'une collaboration entre le secteur public et le secteur privé **(B)**.

A - Cartographie des expérimentations

Analyse chronologique :

D'un point de vue chronologique, il est possible de constater une accélération des expérimentations de la technologie reconnaissance faciale à partir de 2016. En effet, sur quarante-cinq cas recensés, quarante projets ont vu le jour entre 2016 et 2020. Cela s'explique notamment au regard du la course à l'innovation qui se jouent entre les puissances asiatiques et américaines, au sein de laquelle les industriels européens tentent de se frayer un chemin.

92 Surveillance Camera Commissioner, "Statement on the High Court judgment on the use of Automatic Facial Recognition technology by South Wales police", 11 septembre 2019, https://www.gov.uk/government/publications/the-use-of-facial-recognition-technology-by-south-wales-police/statement-on-the-high-court-judgment-on-the-use-of-automatic-facial-recognition-technology-by-south-wales-police

93 Biometrics Commissioner, "Biometrics Commissioner response to court judgment on South Wales Police's use of automated facial recognition technology", 10 septembre 2019, https://www.gov.uk/government/news/automated-facial-recognition

94 T. Blancmont, « Aéroport de Bruxelles : reconnaissance faciale et Dashboard » [en ligne], Air journal, 11 juillet 2019, [consulté le 14/01/2019], https://www.air-journal.fr/2019-07-11-aeroport-de-bruxelles-reconnaissance-faciale-et-dashboard-5213706.html

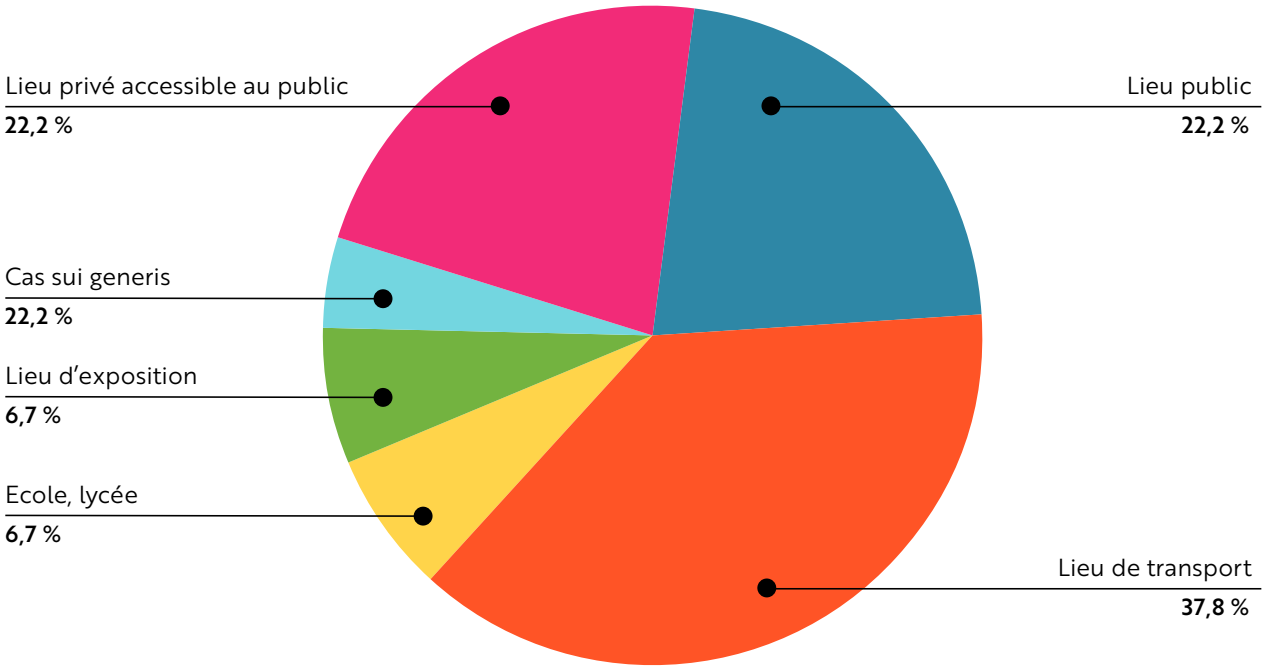
Chronologie des expérimentations par pays						
Pays	**Lieux publics**	**Lieux de transports**	**Établissements d'enseignement**	**Lieux d'exposition**	**Lieux privés ouverts au public**	**Cas *sui generis***
Allemagne		**2017-2018** *Safety Station Südkreuz*				
Belgique		**2015** Expérimentation, aéroport Bruxelles-National **2019** Projet en réflexion, aéroport Bruxelles-National)			**2019** Expérimentation au stade *Racing White Daring Molenbeek*)	
Espagne	**2019** Mise en place d'un nouveau système d'entrée et de sortie du territoire adossé à de la reconnaissance faciale à la frontière hispano-marocaine)	**2019** Application mobile proposée par une compagnie aérienne nationale afin de faciliter l'embarquement des passagers grâce à la reconnaissance faciale	**2019** Utilisation de reconnaissance faciale par un institut public pour contrôler la fréquentation scolaire			
France	**2019** Expérimentation dans le cadre du carnaval de Nice)	**2009-2020** Mise en place pérennisée du système PARAFE dans différents aéroports français (Charles De Gaulle, Orly,Marseille-Provence)	**2017-2020** Projet de mise en place d'un dispositif dans les lycées (ampère / eucalyptus)		**2020** Réflexion et tests internes à l'entreprise pour la mise en place de la reconnaissance faciale au sein du Stade de Metz	
Italie	**2017** Fourniture d'un logiciel de reconnaissance faciale en direct (Sari Realtime) et en différé (Sari Entreprise) à la police pour ses enquêtes	**2014-2019** Installation de dispositifs eGates dans de nombreux aéroports italiens pour le contrôle aux frontières extérieures **2017** Projet d'utiliser la reconnaissance faciale afin de mesurer l'afflux des passagers à l'aéroport Roma Fiumicino **2019-2020** Expérimentation de la reconnaissance faciale à l'embarquement aux aéroports Roma Fiumicino et Milano Linate				

Pays-Bas	**2016** Le centre national de la police judiciaire adopte le logiciel de reconnaissance faciale "MorphoBis" de la Société Safran Identity & Security **2016** Le Centre de biométrie du Service national de coopération opérationnelle met en place un système de reconnaissance faciale "CATCH" qui est adopté par les forces de police (également sur leur bodycam)				**2017** Mise en place de la reconnaissance faciale couplée à de l'apprentissage automatique (Panasonic) dans la grande surface alimentaire *Jumbo Ten Brink Fooda,*pour lutter contre le vol à l'étalage.	
République tchèque					**2019** Projet de mise en place de la reconnaissance faciale à l'entrée des stades. L'autorité de contrôle n'a pas autorisé la mise en oeuvre dudit projet	**2019** Pérennisation : Mise en place de système de reconnaissance faciale au sein d'un chantier de construction. Le projet a été autorisé par l'autorité de contrôle

(Suite)

Royaume-Uni	**2016-2019** Expérimentation par le Met dans les rues de Londres **2016** Experimentation, Carnaval de Nothing Hill **2017** Expérimentation, Carnaval de Nothing Hill **2020** Volonté exprimée de généraliser à Londres pour l'identification des personnes recherchées pour "délits graves"	**2012** Utilisation de la reconnaissance faciale pour le contrôle aux frontières, aéroport de Londres-Heathrow **2017** Expérimentations par les compagnies membres de l'alliance Oneworld de la reconnaissance faciale à l'ensemble des contrôles , aéroport de Londres-Heathrow **2017** (Installation de dispositifs eGates dans la gare Saint Pancras de Londres pour assurer le contrôle aux frontières du Royaume-Uni) **2018** Expérimentation par Easyjet, aéroport de Londres-Gatwick) **2019** Expérimentation généralisée de la reconnaissance faciale, aéroport de Londres-Gatwick) **2019-2020** Expérimentation généralisée de la reconnaissance faciale généralisée, aéroport de Londres-Heathrow		**2018** Expérimentation par la police des Galles du Sud au Motorpoint Arena lors d'un salon d'exposition sur la défense **2018** Installation à titre préventif de caméras équipées d'une solution de reconnaissance faciale au *World Museum* de Liverpool **2019** Dénonciation de l'utilisation de la reconnaissance faciale à des fins de surveillance au *Millenium Point* de Birmingham	**2017** Expérimentation lors de la finale de la Ligue des Champions, le tournoi des Six Nations et les concerts de Kasabian et Liam Gallagher au stade de Cardiff + Expérimentation à Queen's Street à Cardiff **2018** Critique de l'expérimentation, centre commercial *Trafford Centre* à Londres **2018** Expérimentation au centre commercial *Meadowhall* à Sheffield **2019** Expérimentation, centre commercial *Westfield* à Londres	**2016-2018** Expérimentation par la police de Camdem à King's Cross)

Suède	**2019** Pérennisation de la reconnaissance faciale site à une expérimentation de la reconnaissance faciale par les services de police suédois, l'autorité de contrôle a autorisé son utilisation	**2019** Projet avorté (refus de l'autorité de contrôle) de mise en place de la reconnaissance faciale au sein de l'aéroport de Skavsta pour le contrôle des frontières extérieures)	**2018** Projet expérimental d'utilisation de la reconnaissance faciale dans un lycée de Skellefteå. L'autorité de contrôle a interdit la poursuite.			
Danemark					**2019** Le club de Brøndbyernes IF Fodbold A / S - est autorisé à traiter des données biométriques à l'aide de la reconnaissance faciale	
Finlande		**2017** Expérimentation du logiciel de reconnaissance faciale de la société Futurice par la compagnie aérienne Finnair lors de l'enregistrement des passagers à l'aéroport d'Helsinki			**2013** Uniql propose un système de reconnaissance faciale comme mode de paiement	
Slovénie		**2019** Utilisation de la reconnaissance faciale à l'embarquement à l'aéroport de Ljubljana				
TOTAL /45	**10** (2016-2020)	**17** (2009-2020)	**3** (2018-2020)	**3** (2018-2019)	**10** (2013-2020)	**2** (2016-2019)



- **Lieux de transit des personnes**

Le tableau ci-dessus indique que l'introduction de la reconnaissance faciale dans l'espace public – compris ici comme tout lieu de passage ou de rassemblement accessible à tous, indépendamment de la qualité du domaine (public ou privé) – s'est d'abord manifestée dans les lieux de transit de personnes (aéroport, gares, station de métro, etc.). Politiquement, le déploiement de la technologie y a été était défendu par la concentration des personnes qu'ils accueillent et les risques pesant sur leur sécurité de ces personnes. La menace terroriste à la suite des attentats de Londres Paris, Bruxelles et Nice a particulièrement été invoquée. De nombreux Etats se montrent sensible à cette question : parmi les douze pays étudiés, neuf ont expérimenté cette technologie dans ces conditions, ce qui représente les trois-quarts des pays étudiés.

Les usages de la technologie en ces lieux sont divers :

- Les premières expérimentations recensées sur ce terrain visent d'abord un objectif de **contrôle des frontières**.
  La France en constitue un bon exemple : le dispositif PARAFE (Passage automatisé rapide des frontières extérieures) a été mis en place dans plusieurs aéroports stratégiques, dès 2009, pour contrôler les passages aux frontières extérieures de l'espace Schengen. Aujourd'hui, la pratique - subordonnée à une conservation restreinte des données biométriques une fois l'authentification effectuée- est largement observée en **France**[95], au **Royaume-Uni**[96] ou en **Italie**[97]. En **Suède** toutefois, un projet a été refusé par l'autorité de protection : cela tenait à la spécificité du cas d'espèce, le dispositif suédois ne prévoyant pas une suppression immédiate des données biométriques après authentification, mais une conservation en vue d'entraîner l'algorithme[98].

- La généralisation du contrôle aux frontières automatisé par reconnaissance faciale dans les plus grands aéroports européens, tels que Londres-Healthrow ou Paris-Charles de Gaulle, a rapidement suscité l'intérêt des compagnies aériennes pour développer leur propre usage de la technologie. D'autres expérimentations ont donc été initiées par ces compagnies en vue de proposer des **processus d'auto-embarquement** avec des dispositifs d'authentification par reconnaissance faciale. Cet usage

95 Voy. *infra* (France)

96 Voy. *infra* (Italie)

97 Voy. *infra* (Royaume-Uni)

98 Voy. *infra* (Suède), Datainspektionen, « Lagändring krävs för att polisen ska kunna utföra testverksamhet av ansiktsverifiering på flygplats », 16 décembre 2019, https://www.datainspektionen.se/nyheter/lagandring-kravs-for-att-polisen-ska-kuna-utfora-testverksamhet-av-ansiktsverifiering-pa-flygplats/

représente huit des dix-sept cas recensés dans les lieux de transport, soit près de la moitié, répartis entre la **Belgique, l'Espagne, l'Italie, le Royaume-Uni, la Finlande et la Slovénie**. L'objectif poursuivi est ici différent : il s'agit de d'améliorer l'efficacité et la fluidité de l'embarquement des passagers, mais aussi de réduire le personnel au sol[99].

- Un dernier usage de la reconnaissance faciale dans les lieux de transport : **l'identification de comportements suspects ou de personnes recherchées** par **les forces de police**. Le seul cas expérimenté à ce jour sur le terrain l'a été en Allemagne au sein de la Deutsche Bahn[100]. La police belge a, de son côté, manifesté sa volonté d'équiper les caméras de l'aéroport Bruxelles-National afin de pouvoir identifier des suspects en matière de terrorisme et de criminalité organisée, sur place et en temps réel. Ce projet a toutefois été ralenti par la prise de position de l'Organe de l'information policière[101].

En sus d'être les premiers lieux à avoir introduit la reconnaissance faciale pour maintenir l'ordre public, les aéroports et les gares sont également les espaces concentrant le plus grand nombre d'expérimentations pérennisées. Parmi les quarante-cinq expérimentations recensées, dix-sept concernaient les lieux de transports, soit un peu plus d'un tiers des expérimentations européennes, et seuls deux projets ont été avortés en Suède et en Belgique comme précédemment mentionné.

Les lieux de transit constituent un terrain d'expérimentation privilégié pour deux raisons :

- *Premièrement*, la technologie de reconnaissance faciale expérimentée vise à authentifier les personnes au regard de leur pièce d'identité ou de leur carte d'embarquement, c'est-à-dire vérifier que la personne est bien celle qu'elle prétend être. Or, la reconnaissance faciale comme moyen d'authentification est l'usage de la technologie le moins controversé, puisqu'il ne nécessite ni la constitution d'une base de données antérieure ni la conservation des données biométriques récoltées. Au contraire, ces données peuvent être instantanément supprimées une fois la comparaison avec le document officiel effectuée. Tout ceci diminue donc grandement les risques d'atteintes pour les droits et libertés des individus souvent associés à la reconnaissance faciale.
- *Deuxièmement*, ces expérimentations choisissent la base légale du consentement, ce qui limite nettement les incertitudes réglementaires, le régime du consentement étant celui le plus encadré par le RGPD. Elles résultent ainsi d'une démarche volontaire du voyageur.

Ces expérimentations ont donc souvent constitué une prémisse aux autres qui s'en sont suivies : nous constatons que sur dix pays ayant déployé la reconnaissance faciale dans les lieux de transport, sept ont postérieurement entrepris d'autres expérimentations dans l'espace public.

- **Lieux publics**

A la différence de l'« espace public » que nous interprétons largement, nous entendons par « lieu public », les espaces découverts accessibles par toute personne sans restriction. Il s'agit ds expérimentations dites « de plein rue ».

Parmi les douze pays étudiés, six ont expérimenté la reconnaissance faciale en des lieux publics. Aucun d'entre eux n'a toutefois réalisé sa première expérimentation de la technologie dans un espace découvert librement accessible, exception faite des Pays-Bas qui utilisent depuis 2016 des caméras corporelles portées par les

99 Comme l'a défendu l'alliance Oneworld Voy. *infra* (Royaume-Uni), S. Leblal, « La reconnaissance faciale se déploie aux portes d'embarquement à Heathrow » [en ligne], *Le monde informatique*, 10 avril 2017, [consulté le 17/03/2020], https://www.lemondeinformatique.fr/actualites/lire-la-reconnaissance-faciale-se-deploie-aux-portes-d-embarquement-a-heathrow-67889.html

100 Voy. *infra* (Allemagne)

101 Voy. *infra* (Belgique), T. Blancmont, « Aéroport de Bruxelles : reconnaissance faciale et Dashboard » [en ligne], *Air journal*, 11 juillet 2019, [consulté le 14/01/2019], https://www.air-journal.fr/2019-07-11-aeroport-de-bruxelles-reconnaissance-faciale-et-dashboard-5213706.html,

agents de police[102]. Les cinq autres Etats ont tous expérimenté la reconnaissance faciale sur un autre espace public, avant de tester un déploiement en lieu découvert.

Les lieux publics ont fait l'objet de nombreuses expérimentations : dix projets élaborés entre 2016 et 2020 et réparti sur six pays, pour un total de quarante-cinq cas recensés sur douze pays. Les lieux publics comptent ainsi parmi les trois terrains d'expérimentation privilégiés.

Trois cas d'usages se distinguent en ces lieux :

- *Dans un premier temps*, la reconnaissance faciale a été mobilisée pour **« sécuriser » des événements festifs réunissant un grand nombre d'individus**, à l'instar des carnavals de Nothing Hill[103] ou de Nice[104]. Si le premier a uniquement testé la reconnaissance faciale comme moyen d'identification de personnes recherchées, le second a de surcroît testé la technologie pour contrôler et authentifier les personnes accédant à l'évènement[105].
- *Dans un deuxième temps*, la reconnaissance faciale a été mobilisée en des lieux public pour **contrôler l'accès aux frontières**, comme c'est le cas au poste de frontière de Sebta en Espagne[106].
- *Dans un dernier temps*, quatre pays ont expérimenté la reconnaissance faciale pour un **usage policier** afin d'identifier les personnes recherchées en temps direct, comme testé en Italie, aux Pays-Bas et au Royaume-Uni, ou en temps différé par l'intermédiaire des caméras de vidéosurveillance, comme autorisé en Suède ou en Italie.

- **Lieux d'expositions**

Les lieux d'expositions ont également expérimenté des dispositifs de reconnaissance faciale. Les cas recensés se concentrent au Royaume-Uni qui est le seul pays, parmi les douze étudiés, à avoir mené trois expérimentations de la technologie, chacune dans un lieu d'exposition distinct[107].

Notons que ces expériences ont pris des formes différentes :

- Dans certains cas, elles furent **initiées par la police**,et rejoignent donc la catégorie « sécurisation d'événements officiels ». Tel fut le cas au centre d'exposition couvert *Motorpoint Arena* de Cardiff, en mars 2018. Les forces de l'ordre ont justifié l'utilisation de la reconnaissance faciale à l'aune des perturbations de l'évènement par des militants lors des éditions précédentes[108].
- Dans d'autres, le **musée** recourt à la technologie de sa propre initiative.
  Ainsi, en 2018, le *World Museum* de Liverpool a installé un dispositif de reconnaissance faciale « par mesure de précaution au cas où la menace terroriste s'intensifierait avant ou pendant l'exposition *China's First Empereur and the Terracotta Warriors* ». Notons toutefois qu'aucun usage de cette technologie n'aurait finalement été faite d'après le musée[109].

---

102 Voy. *infra* (Pays-Bas), W. Van Gaal, "Gezichtsherkenning op de Nederlandse straten: moeten we dat willen?" [en ligne], *Vice*, 18 juillet 2019, [consulté le 14/01/2020], https://www.vice.com/nl/article/8xzydz/gezichtsherkenning-op-de-nederlandse-straten-moeten-we-dat-willen

103 Voy. *infra* (Royaume-Uni)

104 Voy. *infra* (France)

105 Et consentantes pour participer à l'expérimentation, *Ibidem.*

106 Voy. *infra* (Espagne)

107 Voy.. *infra* (Royaum-Uni)

108 High Court of Justice, Cardiff, précédemment cité, §13

109 Voy.. *infra* (Royaum-Uni), What Does They Know, « FOI request 19/06 », [en ligne], *National Museums Liverpool*, 13 septembre 2019, [consulté le 18/03/2020], https://www.whatdotheyknow.com/request/597557/response/1431227/attach/3/FoI%20No.19%2006.pdf?cookie_passthrough=1

- **Établissements d'enseignement**

Les expérimentations de la technologie de reconnaissance faciale dans les établissements d'enseignement demeurent à ce jour les plus rares.

Tout comme dans les lieux d'exposition, nous n'avons recensés que trois cas, répartis dans trois pays distincts, parmi les quarante-cinq expérimentations totales étudiées. En revanche, à la différence des lieux d'expositions, seule une expérimentation a pu être déployée sur le terrain, dans un établissement scolaire espagnol[110]. Les deux autres cas sont restés à l'état de projet : cela tient en partie aux obstacles juridiques mis en lumière par les décisions suédoise[111] et française[112] analysées ci-après.

Dans ces lieux, la reconnaissance faciale peut être mobilisée pour deux usages :

- L'authentification des élèves à l'entrée de l'établissement, notamment pour contrôler la fréquentation scolaire ;
- L'identification et le suivi des individus afin de détecter des déplacements non autorisés dans l'établissement.

- **Lieux privés accessibles au public**

Les expérimentations de la technologie de reconnaissance faciale dans les lieux privés accessibles au public sont assez nombreuses. Nous avons ainsi relevé dix expérimentations dans ces lieux sur un total de quarante-cinq tout lieu confondu, ce qui représente environ une expérimentation sur cinq. Chacune de ces dix expérimentations sont également réparties entre celles réalisées dans des stades et celles mises en place dans des zones commerciales.

➨ *Expérimentations dans les stades*

L'intérêt du recours à la reconnaissance faciale dans les stades est un phénomène assez récent, accru depuis 2019. Sur douze pays, cinq ont tenté d'expérimenter cette technologie sur ce terrain.

Nos recherches ont permis d'identifier deux cas d'usages distincts :

- Soit les expérimentations menées se cantonnent à l'entrée du stade pour un usage de la technologie comme **moyen d'authentification** des **supporters** consentants. L'expérimentation belge du stade de de Molenbeek[113] ayant, par exemple, mis en place une file prioritaire pour ses abonnés en constitue l'unique illustration.
- Soit la technologie est mobilisée dans l'enceinte même du stade, comme **moyen d'identifier** les **individus interdits d'accès**. Cet usage apparaît comme l'usage le plus sollicité, puisqu'il représente quatre cas parmi les cinq relevés dans les stades. Il apparaît toutefois contesté : accepté au Danemark[114] et au Royaume-Uni[115], il a été prohibé par l'autorité de la protection des données tchèque[116]. La France sera probablement amenée à se prononcer sur la question, le FC Metz ayant fait part de son intérêt pour cet usage[117].

110 Voy. *infra* (Espagne)

111 Voy. *infra* (Suède), Datainspektionen, "Tillsyn enligt EU:s dataskyddsförordning 2016/679 – ansiktsigenkänning för närvarokontroll av elever", précédemment cité

112 Voy. *infra* (France), TA Marseille, 27 février 2020, n°1901249

113 Voy. *infra* (Belgique), B. Schmitz, précédemment cité

114 Voy. *infra* (Danemark)

115 Voy. *infra* (Royaume-Uni)

116 Voy. *infra* (République Tchèque)

117 Voy. *infra* (France), J-L Mounier, « La reconnaissance faciale au FC Metz, une expérimentation qui suscite la controverse » [en ligne], 2 février 2020, [consulté le 18/03/2020], https://www.france24.com/fr/20200202-la-reconnaissance-faciale-au-fc-metz-une-exp%C3%A9rimentation-qui-suscite-la-controverse

➨ *Expérimentations dans les centre commerciaux*

Les expérimentations dans les centres commerciaux - ou à usage commercial - sont au nombre de cinq, réalisées entre 2013 et 2018, dont trois sont concentrées sur le sol britannique.

Ces expérimentations sont mentionnées dans le cadre du présent rapport car elles reposent sur une collaboration rapprochée entre les acteurs privés et les forces de police :

- Une telle expérimentation a été conduite aux Pays Bas, au sein de la grande surface alimentaire *Jumbo Ten Brink Fooda* pour « lutter contre le vol à l'étalage par le biais de grands sacs de course en collaboration avec la police »[118].
- Trois expérimentations britanniques procèdent également d'une collaboration étroite entre un centre commercial privé et la police à *Westfield*, *Trafford Centre* et *Meadowhall*. L'objectif affiché était l'amélioration de la sûreté et de la sécurité du personnel et des clients grâce à l'identification de personnes recherchées ou disparues[119].

Au-delà des collaborations techniques entre les pouvoirs publics et les prestataires privés analysées ci-après, ces cas sont les témoins de la porosité du critère de maintien de l'ordre public.

B - Collaborations public/privé

Le recours à des prestataires privés par les pouvoirs publics dans le cadre des projets de déploiement de la reconnaissance faciale interroge, au regard des risques que présente la technologie sur les droits et libertés des individus d'une part, de l'indépendance des acteurs publics de l'autre.

Bien que nombre d'États recourent à des entreprises européennes pour déployer leurs dispositifs, plusieurs logiciels sont fournis par des opérateurs privés étrangers[120]. Ce constat soulève des interrogations:

- D'une part celle de savoir comment garantir effectivement le droit à la protection des données personnelles des ressortissants européens en cas de recours à un prestataire étranger établit en dehors de l'Union européenne. La législation européenne, le RGPD en particulier, prévoit des dispositifs visant à encadrer les transferts transfrontaliers de données hors de l'Union européenne (décisions d'adéquation, règles d'entreprises contraignantes, etc.)[121]. En tout état de cause la présence du prestataire en dehors des frontières européennes rend son encadrement difficile.

- D'autre part, le recours à des prestataires étrangers dans le cadre de l'usage de la reconnaissance faciale à des fins policières suppose de s'interroger sur les risques d'ingérence et de la sécurité des données si celles-ci sont stockées sur des bases de données situées en dehors de l'Union[122]. Les implications en matière de sécurité nationale sont importantes et nécessitent d'être prise en compte par les États européens dans leurs projets de déploiement de la reconnaissance faciale à des fins policières et sécuritaires.

Seuls deux États ont entrepris de développer la technologie *in house* :

⇨ La **Police suédoise**[123], lors de sa consultation devant l'autorité de protection des données pour la mise

118 Voy. *infra* (Pays-Bas), Panasonic, "Panasonic helps to make JUMBO stores safer / Netherlands" [en ligne], *Panasonic*, [consulté le 15/01/2020], https://security.panasonic.com/case_studies/case151/

119 Voy. *infra* (Royaume-Uni)

120 Voy. *Infra* (Prestataires techniques)

121 Voir Chapitre V du RGPD et de la Directive Police-Justice

122 Ministère de l'Intérieur, « Les risques liés à l'hébergement des données dans les data centers / le cloud » [en ligne], *Flash 35*, septembre 2017, [consulté le 01/02/2020], https://www.prefectures-regions.gouv.fr/ile-de-france/content/download/38300/258289/file/FI%20N%C2%B035%20SEPTEMBRE%20-%20Les%20risques%20li%C3%A9s%20%C3%A0%20l%E2%80%99h%C3%A9bergement%20des%20donn%C3%A9es%20dans%20les%20data%20centers%20et%20le%20cloud.pdf

123 Datainspektionen, Lagändring krävs för att polisen ska kunna utföra testverksamhet av ansiktsverifiering på flygplats, 16 décembre 2019, https://www.datainspektionen.se/nyheter/lagandring-kravs-for-att-polisen-ska-kunna-utfora-testverk-

en place d'un dispositif de reconnaissance faciale au sein de l'aéroport de Skavsta. Le projet avait pour ambition d'entraîner et développer un algorithme de reconnaissance faciale par ses propres services, en vue d'un usage ultérieur généralisé pour le contrôle des frontières extérieures.
Le projet n'a cependant pas été autorisé par le régulateur, les garanties présentées étant jugées insuffisantes.

- ⇨ Aux **Pays-Bas**, les autorités de police lors de la mise en œuvre du système CATCH se sont appuyées sur la solution proposée par le Centre de biométrie de l'Office national de coopération opérationnelle[124].

Le recours à des prestataires privés, y compris pour des missions de police et de sécurité nationale, demeure donc le principe.

Ci-dessous, la liste des prestataires privées qui ont fourni les dispositifs de reconnaissance faciale dans le cadre des expérimentations conduites.

Le tableau ci-dessous recense les différentes nationalités des prestataires techniques mobilisées dans le cadre des expérimentations étudiées.

samhet-av-ansiktsverifiering-pa-flygplats/

124 Dienst Landelijke Operationele Samenwerking, Traduit par nous.

PAYS	Opérateurs privés				
Allemagne -> En **bleu**, les entreprises ayant participé à l'étude de marché -> En **rouge**, les entreprises ayant participé au processus (Berlin Südkreuz)	**Dell EMC AG** Fournisseur du logiciel de reconnaissance faciale *"BioSurveillance"* (USA) **Elbex GmbH** fournisseur du logiciel de reconnaissance faciale *"Anyvision"* (Allemagne) **Ströer Media Deutschland GmbH** Assure le marquage au sol (Allemagne)	**OT Morpho GmbH** (devenu IDEMIA AG durant le projet, fournisseur du logiciel de reconnaissance des visages *"MVI"* (France) **Roth ITK GmbH** fournisseur du système transpondeur (Allemagne)	**Fujitsu** *Greenages Citywide Surveillance* (Japon) **MicroFocus** *IDOL* (UK) **Briefcam** *Briefcam Insight and Protect* (Israël)	**Hitachi** *Hitachi Video Analytics - HVA* (Japon) **Get2Know** *Situational Awareness Builder* (Allemagne)	**IBM** *Intelligent Video Analytics - IVA* (USA) **Securiton** *IPS Public Transport Protection* (Suisse)
Danemark	n/a				
Espagne	**Cas n°1 (école) :** n/a	**Cas n°2 (frontière) :** n/a	**Cas n°3 (aéroport) :** **Ibéria** : Iberia Líneas Aéreas de España, compagnie nationale espagnole basée à l'aéroport international de Madrid-Barajas		
Finlande	**Cas n°1 (paiement dans zones commerciales) :** Uniql (Finlande)	**Cas n°2 (aéroport) :** Futurice (Finlande)			
France	**Cas n°1 (Carnaval) :** Confidentia (Monaco) proposant la solution Anyvision (Israël)	**Cas n°2 (Lycées) :** Cisco (USA)	**Cas n°3 (Aéroports) :** Gemalto (Pays-Bas)	**Cas n°4 (Stade de Metz) :** TWO-I (France)	

Italie	**Cas n°1 (SARI)** Parsec 3.26 (Lecce) Instituto di Scienze Applicate e Sistemi Intelligenti	**Cas n°2 (contrôles aux frontières aux aéroports de Venise et Trévise)** Naitec (Vénétie)	**Cas n°2 (contrôles aux frontières à l'aéroport Roma Fiumicino) :** Société internationale de télécommunication aéronautique (Genève)	**Cas n°2 (contrôles à l'aéroport de Naples)** Consortium réunissant NTT data (Japon) Indra (Espagne) Secunet (Allemagne) Studio FRA (Italie)	**Cas n°3 (embarquement à l'aéroport de Roma Fimucino)** Vision Box (Portugal) **Cas n°3** - embarquement à l'aéroport Milano Linate n/a
Pays-Bas	**Cas n°1** : Safran Identity & Security (renommée IDE-MIA : France)	**Cas n°2 :** Centre de biométrie du Service national de coopération opérationnelle (DLOS : Centrum voor Biometrie van de Dienst Landelijke Operationele Samenwerking) pour le système CATCH (Pays-Bas)	**Cas n°3 :** Panasonic (Japon) pour reconnaissance faciale dans la grande surface alimentaire Jumbo Ten Brink Fooda		
Royaume-Uni	Solution NeoFace de l'entreprise NEC	Vision-Box	Collaboration entre les sociétés Atkins (Royaume-Uni) et Aurora (Royaume-Uni)		
Slovénie	Amadeus (Espagne) Gemalto (Pays-Bas)				
Suède	**Cas n°1 :** n/a	**Cas n°2 :** n/a	**Cas n°3 :** n/a		
Belgique	**Cas n°1**: n/a	**Cas n°2** : Zetes (Belgique) utilisant la solution de Panasonic (Japon)			
République tchèque	**ConVision** *Face ID* (Entreprise tchèque) -> Chantier	**Panasonic** (Japon) -> Stades			

Pays	Prestataires nationaux	Prestataires européens	Prestataires hors Union Européenne
Allemagne	✓	Français, anglais et suisses	Japonais et américains
Belgique	✓		Japonais
Danemark	n/a	n/a	n/a
Espagne	✓	n/a	n/a
Finlande	✓		
France	✓	Monégasques et néerlandais	Israéliens et américains
Italie	✓	Espagnols et portugais allemands	Japonais
Pays-Bas	✓	Français	Japonais
République Tchèque	✓		Japonais
Royaume-Uni	✓	Portugais	Japonais
Slovénie		Espagnols et néerlandais	
Suède	n/a	n/a	n/a

Notre étude met en exergue la prédominance des industriels européens sur le marché de la reconnaissance faciale en Europe. Ce constat est encourageant au regard d'une application effective de la législation européenne en matière de protection des données personnelles.

Les entreprises israéliennes, américaines et japonaises demeurent présentes sur le marché, mais sont moins nombreuses que leurs homologues européennes.

Les entreprises chinoises enfin, dominantes dans les classements internationaux, sont peu présentes, voir absente au sein de l'Union. Aucun des cas évoqués dans le rapport ne fait état de l'utilisation d'une technologie de reconnaissance faciale chinoise.

III. Résistance et recours

À ce jour, aucun recours n'a été introduit par un particulier contre le déploiement de la reconnaissance faciale dans l'espace public auprès d'une autorité de contrôle dans les pays étudié. Leurs prises de positions consistent principalement en la publication de lignes directrices, d'avis ou de délibérations trouvant leur origine dans une procédure d'auto-saisine.

Les décisions juridictionnelles sont encore, à ce jour, peu nombreuses : seules deux juridictions se sont prononcées, en France[125] et au Royaume-Uni[126] .

125 TA Marseille, 27 février 2020, n°1901249. **Voy**. *infra* France.

126 High Court of Justice, Cardiff, précédemment cité Voy. *infra* Royaume-Uni.

⇨ Au **Royaume-Uni**, deux recours ont été introduits dans le but de contester des expérimentations menées par la police des Galles du Sud ; ils ont donné lieu à une décision de la High Court de Cardiff. Cette dernière a reconnu la légalité des dispositifs : les pouvoirs généraux de police constituent une base légale suffisante pour réaliser un traitement de données biométriques et que ce dernier est assorti de garanties [127]. L'appel est pendant.

Un autre recours introduit par l'association de défense des libertés publiques Big Brother Watch et de Jenny Jones, une représentante de la Chambre des Lords [128] est pendantdevant la High Court de Londres [129].

⇨ En **France**, un recours contestant une expérimentation au sein d'établissement scolaire a conduit le juge administratif à se prononcer. Le tribunal administratif de Marseille n'a pas admis la légalité de l'expérimentation[130] du déploiement de portiques dotés de solution de reconnaissance faciale dans deux lycées de la région Provence-Alpes-Côte-d'Azur [131].

Les recours contre les dispositifs de reconnaissance faciale dans l'espace public en Europe		
Pays	**Recours devant le juge**	**Recours devant l'autorité de contrôle**
Allemagne	Aucun	Aucun
Belgique	Aucun	Aucun
Danemark	Aucun	Aucun
Espagne	Aucun	Aucun
Finlande	Aucun	Aucun
France	Recours devant le tribunal administratif de Marseille : **TA Marseille, 27 février 2020, n°1901249**	Aucun
Italie	Aucun	Aucun
Pays-Bas	Aucun	Aucun
Royaume-Uni	Recours devant la High Court de Cardiff : **High Court of Justice, Cardiff, *R (Bridges) v. CCSWP and SSHD*, [2019] EWHC 2341 (ADMIN)**. La procédure est en appel. Recours pendant devant la High Court de Londres	Aucun
République-Tchèque	Aucun	Aucun
Slovénie	Aucun	Aucun
Suède	Aucun	Aucun
TOTAL	**Deux décisions de justice et un recours pendant**	**Aucun recours**

127 Voy. *infra* (Royaume-Uni)

128 Big Brother Watch, "Stop the Met Police using authoritarian facial recognition cameras" [en ligne], *Crowdjustice* [consulté le 20/03/2020], https://www.crowdjustice.com/case/face-off/

129 J. Jones, publication Twitter de Jessy Jones, 29 janvier 2020, 6:45 a.m, [consulté le 20/03/2020], https://twitter.com/GreenJennyJones/status/1222395308082126849?s=20

130 Pour des motifs tenant tant à la légalité externe qu'à la légalité interne. Voy. *infra* (France)

131 Voy. *infra* (France)

Reconnaissance de la légalité des expérimentations de la reconnaissance faciale dans l'espace public menée en Europe		
Décision de justice	**Légalité du dispositif**	**Principaux motifs**
TA Marseille, 27 février 2020, n°1901249	Non	Incompétence de la région ; consentement non valide
High Court of Justice, Cardiff, *R (Bridges) v. CCSWP and SSHD*, [2019] EWHC 2341 (ADMIN)	Oui	Compétence de la police sur le fondement de ses pouvoirs généraux ; existence de garanties

Il n'existe pas de consensus sociétal sur la question de la reconnaissance faciale, le contentieux émergent en témoigne. En France comme au Royaume-Uni, ils s'inscrivent dans le cadre d'un contentieux stratégique, initiés par les associations de défense des libertés (La Quadrature du Net, la Ligue des Droits de l'Homme[132], Big Brother Watch et Liberty) et de personnalités engagées (Edward Bridges, Jenny Jones). La présence de syndicats d'enseignants et de fédération de parents d'élèves constitue à ce jour une particularité française - ces derniers n'ayant pas introduit ou soutenu de recours au Royaume-Uni - qui peut s'expliquer par la nature du projet envisagé à Nice et à Marseille [133].

Ce contentieux stratégique rend compte du déficit de légitimité dont souffre la reconnaissance faciale auprès d'une partie de la population. Au Royaume-Uni, une étude réalisée en ligne par l'institut Ada Lovelace en 2019 [134] - sur un échantillon de 4109 individus âgés de 16 ans et plus - s'intéresse à l'acceptabilité de la reconnaissance faciale auprès du public.

Résultats de l'étude du Ada Lovelace Institute sur l'acceptabilité de la reconnaissance faciale				
Sur la connaissance et l'information du public en matière de reconnaissance faciale				
90% des personnes interrogées disent être conscientes de l'utilisation de la reconnaissance faciale	53% des sondés disent avoir des connaissances sur la technologie	10% des sondés n'ont aucune connaissance en la matière	24% des sondés disent que la technologie utilisée par la police est discriminant	18% des sondés estiment que la technologie est imprécise
Conclusion : La connaissance du public en la matière reste limitée, il est donc suggéré de mettre en place un véritable moratoire en vue de renforcer la base démocratique face aux technologies de reconnaissance faciale, en redonnant à l'individu les connaissances nécessaires.				

132 Voy. *infra* (Interviews)

133 Voy. *infra* (France)

134 Ada Lovelace Institute, "Beyond face value : public attitudes to facial recognition technology" [en ligne], septembre 2019 [consulté le 20/03/2020], https://www.adalovelaceinstitute.org/wp-content/uploads/2019/09/Public-attitudes-to-facial-recognition-technology_v.FINAL_.pdf

Résultats de l'étude du Ada Lovelace Institute sur l'acceptabilité de la reconnaissance faciale		
Sur la possibilité de consentir ou de ne pas consentir à la reconnaissance faciale		
Pour 46% des sondés, les individus devraient avoir l'opportunité de ne pas consentir lorsqu'ils sont confrontés à une technologie de reconnaissance faciale	Pour 28% des sondés, les individus ne devraient pas avoir l'opportunité de ne pas consentir lorsqu'ils sont confrontés à une technologie de reconnaissance faciale	Pour 56% des minorités ethniques, les individus devraient avoir l'opportunité de ne pas consentir lorsqu'ils sont confrontés à une technologie de reconnaissance faciale
Conclusion: Les personnes de couleur sont statistiquement plus sujettes aux inexactitudes et aux discriminations. Concernant le recueil consentement, il y a une nécessité de réduire l'écart existant entre les attentes du public et ce que la loi dispose		

Sur la peur d'une normalisation de la surveillance d'une telle technologie et l'acceptation d'une telle technologie en cas d'utilité avérée				
Pour 70% des sondés, l'utilisation de la reconnaissance faciale devrait être autorisée par la police dans le cadre de ses investigations criminelles	Pour 50% des sondés, la reconnaissance faciale devrait être utilisée dans les aéroports pour remplacer les passeports si l'usage reste proportionné	Pour 80% des sondés, la reconnaissance faciale est bénéfique et contribue à assurer la sécurité de la société	67% des sondés sont mal à l'aise avec l'idée d'un déploiement de la reconnaissance faciale dans les écoles	61% des sondés sont mal à l'aise avec l'idée d'un déploiement de la reconnaissance faciale dans les transports publics
Conclusion : Le public sondé procède lui-même à une balance entre intérêts et bénéfices sécuritaires, et limites à poser face au risque d'une surveillance de tous et un affaiblissement de la vie privée. Par ces enjeux revient l'intérêt d'un débat et d'une éducation accrue des individus en vue d'intégrer pleinement le point de vue citoyen dans cet équilibre des intérêts.				

Sur l'absence de soutien inconditionnel des individus dans l'utilisation de la reconnaissance faciale dans la police		
Pour 55% des sondés, le gouvernement doit poser des limitations strictes pour l'utilisation de la reconnaissance faciale dans des circonstances spécifiques	Pour 71% des sondés, la police doit être capable d'utiliser la reconnaissance faciale dans les espaces publics, à condition qu'elle contribue à réduire la criminalité	29% des sondés sont inconfortables avec l'idée d'une utilisation de la reconnaissance faciale dans un scénario d'utilisation policière
Conclusion : Il existe une forte corrélation entre acceptation de la technologie et impact sur la criminalité. Afin de réduire l'écart entre les attentes du public et l'usage que pourrait en faire la police, il est préconisé par l'institut d'approfondir les efforts régulatoires et d'évaluation en la matière. Chaque usage doit être envisagé en amont et les avis des groupes minoritaires doivent être pris en compte.		

Résultats de l'étude du Ada Lovelace Institute sur l'acceptabilité de la reconnaissance faciale	
Sur la confiance accordée au secteur privé et l'utilisation éthique de la reconnaissance faciale	
77% des sondés sont opposés à l'utilisation de la reconnaissance faciale à des fins commerciales ou de recrutement	70% des sondés estiment que les acteurs privés n'utilisent pas la technologie de manière éthique
Conclusion : Le public manifeste une méfiance pour l'utilisation de la reconnaissance faciale dans les espaces privés tels que les commerces ou les lieux de travail. La finalité sécuritaire et de lutte contre la criminalité seule semble emporter l'adhésion de la majorité des sondés, la confiance ne peut être renforcée qu'avec une transparence et communication accrue entre acteurs privés, citoyens et législateur. Une meilleure sensibilisation du public fournira les armes nécessaires aux individus pour soulever les préoccupations qui méritent d'être intégrées au débat.	

Sur l'importance d'une régulation étatique à l'égard des acteurs privés dans l'utilisation de la reconnaissance faciale				
Pour 50% des sondés, les entreprises privées ne devraient pas vendre de dispositifs de reconnaissance faciale à la police	Pour 55% des sondés, le gouvernement devrait limiter l'utilisation de la reconnaissance faciale par la police	Pour 70% des sondés, le secteur privé ne devrait pas vendre cette technologie aux écoles	Pour 40 % des sondés, le gouvernement devrait interdire l'utilisation de la reconnaissance faciale dans les écoles	Pour 30% des sondés, le gouvernement n'a pas à interdire l'utilisation de la reconnaissance faciale dans les écoles
Conclusion : En vue de garantir une appréhension adéquate par l'opinion publique, il serait opportun pour une partie des sondés d'interrompre le commerce de tels dispositifs par les acteurs privés aux acteurs publics (écoles, police). Cela laisserait plus de place à la correction des défis techniques et discriminatoires que pose la technologie aujourd'hui. Une nouvelle gouvernance s'impose et il est important que la reconnaissance faciale procure des avantages à la fois privés et publics.				

BIBLIOGRAPHIE

I. Législation

A - Lois

- Code de la Sécurité intérieur (article L251-1 à L255-1, ainsi que les articles L223-1 à L223-9 en matière de lutte contre le terrorisme et les atteintes aux intérêts fondamentaux de la nation)
- Lag (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område, https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-20181693-om-polisens-behandling-av_sfs-2018-1693
- Loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance (dite « loi caméras »),http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2007032139&table_name=loi
- Surveillance Camera Code of Practice, Juin 2013, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/282774/SurveillanceCameraCodePractice.pdf

B - Jurisprudence

- High Court of Justice, Cardiff, *R (Bridges) v. CCSWP and SSHD*, [2019] EWHC 2341 (ADMIN), https://www.judiciary.uk/wp-content/uploads/2019/09/bridges-swp-judgment-Final03-09-19-1.pdf
- TA Marseille, 27 février 2020, n°1901249, https://www.laquadrature.net/wp-content/uploads/sites/8/2020/02/1090394890_1901249.pdf

II . Prise de position des autorités régulatrices de la protection des données

- Agencia Española de Protección de Datos, « Orientaciones para centros educativos - Informe sobre la utilización por parte de profesores y alumnos de aplicaciones que almacenan datos en nube con sistemas ajenos a las plataformas educativas », 6 mars 2018, https://www.aepd.es/sites/default/files/2019-09/guia-orientaciones-apps-datos-alumnos.pdf
- Agencia Española de Protección de Datos, « Guía sobre el uso de videocámaras para seguridad y otras finalidades », 29 juin 2018, https://www.aepd.es/sites/default/files/2019-09/guia-videovigilancia.pdf
- Agencia Española de Protección de Datos, « Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD », https://www.aepd.es/sites/default/files/2019-09/guia-analisis-de-riesgos-rgpd.pdf
- Autorité de la protection des données, « Un choix de société », https://www.autoriteprotectiondonnees.be/un-choix-de-soci%C3%A9t%C3%A9
- Biometrics Commissioner, "Response to announcement on Live Facial Recognition", 24 janvier 2020, https://www.gov.uk/government/news/response-to-announcement-on-live-facial-recognition
- CEDP, Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est «susceptible d'engendrer un risque élevé» aux fins du règlement (UE) 2016/679, https://www.cnil.fr/sites/default/files/atoms/files/wp248_rev.01_fr.pdf
- Commission Nationale de l'Informatique et des Libertés, « Liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données n'est pas requise », https://www.cnil.fr/sites/default/files/atoms/files/liste-traitements-aipd-non-requise.pdf

- Datainspektionen, "Polisen får använda ansiktsigenkänning för att utreda brott", 24 octobre 2019, https://www.datainspektionen.se/nyheter/polisen-far-anvanda-ansiktsigenkanning-for-att-utreda-brott/
- Datainspektionen, "Tillsyn enligt EU:s dataskyddsförordning 2016/679 – ansiktsigenkänning för närvarokontroll av elever", 20 août 2019, https://www.datainspektionen.se/globalassets/dokument/beslut/beslut-ansiktsigenkanning-for-narvarokontroll-av-elever-dnr-di-2019-2221.pdf
- Information Commissioner's Opinion, "The use of live facial recognition technology by law enforcement in public places", 31 octobre 2019, https://ico.org.uk/media/about-the-ico/documents/2616185/live-frt-law-enforcement-report-20191031.pdf
- Secrétariat Général de l'Autorité de protection des données, « Adoption de la liste des catégories de traitement devant faire l'objet d'une analyse d'impact relative à la protection des données conformément à l'article 35.4 du Règlement Général sur la Protection des données (CO-A-2018-001) », n°01/2019, 16 janvier 2019, https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/01_2019_SG.pdf

III. Presse numérique

- Ada Lovelace Institute, "Beyond face value : public attitudes to facial recognition technology" [en ligne], septembre 2019 [consulté le 20/03/2020], https://www.adalovelaceinstitute.org/wp-content/uploads/2019/09/Public-attitudes-to-facial-recognition-technology_v.FINAL_.pdf
- Barik S., "Brussels Airport to scrap facial recognition enabled e-gates as the system was 'constantly defective': Report" [en ligne], *Medianama*, 18 février 2020, [consulté le 25/02/2020], https://www.medianama.com/2020/02/223-brussels-airport-facial-recognition-egates-scrapped/
- Big Brother Watch, "Stop the Met Police using authoritarian facial recognition cameras" [en ligne], *Crowdjustice* [consulté le 20/03/2020], https://www.crowdjustice.com/case/face-off/
- Blancmont T., « Aéroport de Bruxelles : reconnaissance faciale et Dashboard » [en ligne], *Air journal*, 11 juillet 2019, [consulté le 14/01/2019], https://www.air-journal.fr/2019-07-11-aeroport-de-bruxelles-reconnaissance-faciale-et-dashboard-5213706.html
- CT24, « Poznala vás kamera, na stadion nemůžete. Ministerstvo chystá zákon proti výtržníkům » [en ligne], *CT24*, 16 février 2020, [consulté le 01/02/2020], https://ct24.ceskatelevize.cz/domaci/3048906-poznala-vas-kamera-na-stadion-nemuzete-ministerstvo-chysta-zakon-proti-vytrznikum
- Ds Avond, "Federale politie moet gezichtsherkenning stopzetten" [en ligne], *De Standaard*, 20 septembre 2019, [consulté le 11/03/2020], https://www.standaard.be/cnt/dmf20190920_04618911?articlehash=78C468B42191245F2A8AF844715B8EC50284A320CD3B402C88EB743AE296BC05D9815613E26EEF112EB4A61FF7E4A0E0769D77397538564A75018A2BF311E6DE
- Dussert M., « Quand Big Brother dérape au carnaval de Notting Hill » [en ligne], *L'adn*, 6 septembre 2017, [consulté le 25/03/2020], https://www.ladn.eu/tech-a-suivre/ia-machine-learning-iot/quand-big-brother-derape-au-carnaval-de-notting-hill/
- Ladiray M., « Biométrie, mobile, automatisation : l'aéroport sera connecté ou ne sera pas » [en ligne], *TOM. travel*, 8 novembre 2019, [consulté le 15/01/2020], https://www.tom.travel/2019/11/08/biometrie-mobile-automatisation-aeroport-sera-connecte-ou-ne-sera-pas/
- Panasonic, "Panasonic helps to make JUMBO stores safer / Netherlands" [en ligne], *Panasonic*, [consulté le 15/01/2020], https://security.panasonic.com/case_studies/case151/

- Schmitz B., « Le RWDM comme laboratoire pour une technologie de reconnaissance faciale » [en ligne], *RTBF*, 5 septembre 2018, [consulté le 14/01/2020], https://www.rtbf.be/info/regions/bruxelles/detail_le-rwdm-comme-laboratoire-pour-une-technologie-de-reconnaissance-faciale?id=10011249
- Van Gaal W., "Gezichtsherkenning op de Nederlandse straten: moeten we dat willen?" [en ligne], *Vice*, 18 juillet 2019, [consulté le 14/01/2020], https://www.vice.com/nl/article/8xzydz/gezichtsherkenning-op-de-nederlandse-straten-moeten-we-dat-willen
- Ville de Nice, Rapport « Expérimentation reconnaissance faciale », 20 juin 2019, https://www.documentcloud.org/documents/6350838-Bilan-Reconnaissance-Faciale.html
- Wessbecher L., « La reconnaissance faciale dans les écoles est-elle vraiment la solution contre les fusillades ? » [en ligne], *France 24*, 11 juin 2018 [consulté le 20/03/2020], https://www.france24.com/fr/20180611-reconnaissance-faciale-ecoles-est-elle-vraiment-solution-contre-fusillades

What Does They Know, « FOI request 19/06 », [en ligne], *National Museums Liverpool*, 13 septembre 2019, [consulté le 18/03/2020], https://www.whatdotheyknow.com/request/597557/response/1431227/attach/3/FoI%20No.19%2006.pdf?cookie_passthrough=1

PARTIE III.
ETUDE PAR ETAT

Cette dernière partie dresse un état des lieux du recours à la reconnaissance faciale dans l'espace public à l'échelon national. Neuf États sont étudiés : la France, la Belgique, l'Espagne, la France, l'Italie, les Pays-Bas, la République tchèque, le Royaume-Uni et la Suède. Accessoirement, nous apportons également – non de manière exhaustive, des informations relatives aux expérimentations conduites au Danemark en Finlande et en Slovénie.

Allemagne

I. Législation

À l'échelon national, l'encadrement légal de la reconnaissance faciale dans l'espace public se dessine à travers la loi nationale sur la protection des données et les lois sur la protection des données des États fédéraux ; ces dispositions gouvernent, pour une large partie, le traitement et l'exposition des données sur le territoire :

- La loi fédérale sur la protection des données du 20 décembre, laquelle a modifié la loi du 21 janvier 1977 portant protection contre l'emploi abusif de données d'identification personnelle dans le cadre du traitement des données (*Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung*)[135]. Elle s'applique indifféremment au secteur public et au secteur privé ;
- La loi d'adaptation de la législation allemande aux dispositions du RGPD, adoptée le 27 avril 2017 par le Bundestag (Bundesdatenschutz – BDSG) ;
- Les lois relatives à la protection des données personnelles dans la législation de chaque État (*Land*), lesquels procèdent à l'adaptation de leurs lois sur la protection des données au RGPD ;

Le législateur allemand a adapté les dispositions nationales relatives à la protection des données et procédé à la mise en œuvre de la directive sur la protection des données à l'égard du traitement des données à caractère personnel par les autorités compétentes aux fins de prévention et de détection des infractions pénales, d'enquête et de poursuite en la matière. À cet égard, la BDSG fut notamment révisée à travers le prisme du règlement UE 2016/680 (loi d'adaptation et de mise en œuvre de la protection des données de l'UE (*DSAnpUG-EU, Datenschutz-Anpassungs-und Umsetzungsgesetz EU*)[136].

La loi d'adaptation précitée complète la réglementation sur la protection des données (RGPD) directement applicable dans les domaines où elle laisse une marge de manœuvre aux États pour leurs propres préférences ou mandats réglementaires. Par ailleurs, la loi fédérale sur la protection des données met en œuvre des parties essentielles de la directive « Police-Justice ».

Enfin, en matière de vidéosurveillance, d'autres dispositions doivent également être observées: la loi fédérale sur la protection des données, la loi de l'État sur la protection des données mais aussi le droit à sa propre image qui est une composante du droit à l'autodétermination informationnelle[137]. Ce droit prend place à l'article 2 au sein de la Loi Fondamentale de la République fédérale d'Allemagne[138].

II. Position des instances compétentes en matière de protection des données.

Nous évoquerons dans un premier temps la position adoptée par l'autorité de contrôle, le Commissaire fédéral à la protection des données (*Die Beauftragte für den Datenschutz und die Informationsfreiheit,* A), puis dans un second, la position de la Commission fédérale d'éthique des données (*Daten Ethik Kommission,* B).

---

135 Loi fédérale sur la protection des données (BDSG) du 30 juin 2017, modifiée par l'article 12 de la loi du 20 novembre 2019.
https://www.gesetze-im-internet.de/bdsg_2018/BJNR209710017.html

136 Deuxième loi d'adaptation de la loi sur la protection des données au règlement (UE) 2016/679 et de transposition de la directive (UE) 2016/680. http://dipbt.bundestag.de/extrakt/ba/WP19/2390/239070.html

137 Arrêt rendu par la Cour constitutionnelle de Karlsruhe le 15 décembre 1983 consacrant un droit à « l'autodétermination informationnelle », attaché à la personne et visant à garantir la capacité d'un individu à décider de la communication et de l'utilisation de ses données à caractère personnel.
https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/1983/12/rs19831215_1bvr020983.html

138 Article 2, Loi fondamentale de la République fédérale d'Allemagne (Grundgesetz für die Bundesrepublik Deutschland).
https://www.gesetze-im-internet.de/gg/art_2.html

A - Position du commissaire fédéral à la protection des données

Le 24 janvier 2019, le Commissaire fédéral à la protection des données appelait à la retenue en matière de reconnaissance faciale[139]. Il considérait qu'à défaut de nouvelle base juridique, l'évaluation biométrique de matériel vidéo était illégale. Le volume de données collectées fait peser le risque sur les individus d'être la cible des autorités, sans même qu'une réglementation limite ces dangers. Selon l'autorité allemande, le sentiment de surveillance peut consciemment et inconsciemment orienter les comportements et dissuader les individus de participer à certaines manifestations pourtant légales. Le Commissaire fédéral à la protection des données et à la liberté de l'information, Ulrich Kelber, réaffirmait ainsi « il n'existe actuellement aucune base légale pour la reconnaissance biométrique automatisée du visage »[140].

Faisant suite au communiqué de septembre 2019 annonçant un investissement supérieur à 130 millions d'euros d'ici 2024 dédié à la reconnaissance faciale, le Commissaire a rappelé la nécessité d'encadrer la reconnaissance faciale et plus largement la collecte des données biométriques dans l'espace public. Sous l'empire du droit allemand, l'adoption d'une nouvelle loi apparaît donc indispensable.

B - Position de la Commission fédérale d'éthique des données

Dans son rapport de décembre 2019[141], la Commission d'éthique plaide en faveur d'un renforcement du cadre juridique actuel, dans un souci de prévention des risques de manipulation ou de discrimination des individus. Le recueil du consentement revêt une importance particulière, notamment pour la sauvegarde du droit à l'autodétermination informationnelle, spécifique à l'Allemagne[142].

La Commission considère que le régime de consentement devrait être soumis à des limitations de fond : l'individu « moyen » se trouve dépassé par la complexité des décisions, enjeux et conséquences des traitements successifs étant souvent ignorés[143]. Elle invite aussi l'État à mettre en place des conditions propices à la navigation des usagers dans le monde numérique sans crainte de ces derniers en la survenance d'un préjudice grave de la part d'autres parties. Ces observations sont d'autant plus essentielles en matière de reconnaissance faciale, impliquant le traitement de données sensibles.

Le rapport suggère encore d'établir des « limites absolues » lorsque les opérations de traitement des données personnelles présentent des dangers pour la vie privée en violation des droits fondamentaux. Le niveau de risque pour les individus est, selon la Commission, maximal dans le cas du recours à la reconnaissance faciale. Elle propose aussi de renforcer le niveau de transparence dans les échanges d'informations (notamment) et met en garde contre l'émergence de réseaux d'informations entre les agences gouvernementales.

Enfin la Commission appelle à l'adoption de garanties supplémentaires et une exploitation restrictive des données biométriques par le gouvernement et toute autorité y ayant recours dans les mesures préventives et/ou répressives.

---

139 Commissaire fédéral à la protection des données et au droit à l'information « *Un délégué fédéral à la protection des données met en garde contre la reconnaissance faciale* », 24 janvier 2019. « *Bundesdatenschutzbeauftragter mahnt Zurückhaltung bei Gesichtserkennung an* ». https://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2019/02_Zur%C3%BCckhaltungbeiGesichtserkennung.html

140 Ulrich KELBER, « Le responsable de la protection des données met en garde contre la reconnaissance automatique des visages », [en ligne], *t3n*, 16 janvier 2019, [consulté le 16/01/2020]. https://t3n.de/news/datenschutzbeauftragter-kelber-1137512/

141 Daten Ethik Kommission, "Opinion of the Data Ethics Commission", 10 octobre 2019. https://www.bmjv.de/SharedDocs/Downloads/DE/Themen/Fokusthemen/Gutachten_DEK_EN_lang.pdf?__blob=publicationFile&v=3

142 Daten Ethik Kommission, *ibidem*. §3.2.1 p. 95.

143 Cette difficulté d'appréhension par l'usager est de surcroît entretenue par les fournisseurs de services numériques, qui procèdent, selon elle, à une utilisation inadéquate du consentement.

III. Cas d'usage

➲ Projet « *Safety Station Südkreuz* »

La principale expérimentation conduite en Allemagne concerne la surveillance des gares. Le projet pilote a été lancé en commun par le ministère de l'Intérieur et la Deutsche Bahn (compagnie ferroviaire allemande dont l'unique actionnaire est la République fédérale) avec la participation de la police fédérale et du bureau fédéral de la police criminelle.

L'expérimentation a commencé en juillet 2017[144]. Elle avait pour objectif de détecter et prévenir les « comportements suspects » dans une gare. Six scénarios de mise en œuvre ont été évoqués par le ministre fédéral, notamment : l'identification des objets/bagages abandonnés, le comptage des individus, une meilleure régulation des flux d'usagers. Les opérateurs caméras avaient aussi la possibilité de marquer les personnes avec leurs vêtements et leurs visages, de sorte que le système puisse les suivre sur une période de temps donnée.

Ce projet d'analyse vidéo est lui-même subdivisé en deux sous-projets :

- ⇨ Le premier sous-projet a vocation à tester l'utilité de la reconnaissance des visages dans les flux vidéo en direct des caméras de surveillance de la *Deutsche Bahn*, et ce, à des fins policières. Précisons que la *Deutsche Bahn* se contente ici de fournir l'infrastructure technique (les caméras) et d'informer les usagers, mais n'est pas chargée de la mise en œuvre de l'expérimentation dévolue à la police.

- ⇨ Le second sous-projet vise à tester des systèmes d'analyse vidéo dits « intelligents » pour le traitement et l'évaluation de divers scénarios de risque par la Deutsche Bahn et la police fédérale. Cette expérimentation a commencé à compter de janvier 2019. La direction de ce sous-projet est assurée par la *Deutsche Bahn*.

1re phase de test

Initialement, les tests étaient effectués durant 6 mois afin d'apprécier la compatibilité d'un dispositif de reconnaissance faciale sur les caméras de la gare, à cet effet, plusieurs dispositifs commercialisés ont été testés et comparés (Idemia, Dell, Elbex, AnyVision). Cette expérimentation a débuté le 1er aout 2017 et s'est poursuivie jusqu'au 31 juillet 2018.

Les visages étaient comparés au sein d'une base de données comprenant les photos de 300 volontaires lesquels avaient reçu des codes de réduction Amazon en échange de leurs données et photos.

2de phase de test

Le Ministère de l'Intérieur identifie les différents acteurs éligibles à poursuivre le projet (Briefcam, Fujitsu, Hitachi, IBM, MicroFocus, Securiton, Get2Know).

Toutes ces entreprises ont mis en œuvre des dispositifs pouvant reconnaître les mouvements anormaux de foule ou les objets abandonnés, toutefois les fonctionnalités sont très différentes entre elles.

Information. Durant la première phase de test, la *Deutsche Bahn* balisait les coins de la gare. Le dispositif de reconnaissance faciale était signalé aux usagers avec des bannières et des signes, toutes les zones de la station étaient accessibles sans besoin de pénétrer dans les zones de détection marquées. Ces précautions témoignent de la volonté d'obtenir le consentement des usagers de manière consciente et éclairée. Il semblerait toutefois que celles-ci ne se retrouvent pas dans la seconde phase du projet.

---

144 Direction générale de la police fédérale, « *Reconnaissance biométrique du visage* » (*Biometrische Gesichtserkennung*) dans le cadre de tests des systèmes d'analyse vidéo intelligents par le ministère fédéral de l'intérieur, le siège de la police fédérale, l'Office fédéral de la police criminelle et la Deutsche Bahn AG à la gare de Berlin Südkreuz [en ligne], 18 septembre 2018, [consulté le 16/01/2020]. https://cutt.ly/RrYnZOx

Bilan.

Le bilan de l'expérimentation est mitigé. L'Office fédéral de la police rapporte les résultats suivants[145] :

- Lors de la 1re phase d'expérimentation, près de 61,000 visages ont été analysés avec un taux de réussite de 68,5% ;
- Lors de la 2de phase d'expérimentation, 41,000 visages qui ont été analysés pour un taux de réussite moyen de 82,8%.

Le rapport de l'office fédéral de police propose des améliorations de nature à accroître la précision du dispositif (amélioration de l'angle des caméras, amélioration de la lumière). Au terme de celle-ci le taux de réussite grimperait à 94,4% en phase de test 1 et 98,2% en phase de test 2.

D'autres études[146] affirment que les caméras de Südkreuz auraient reconnu à tort plus d'une personne sur deux cents. Un expert de l'institut Fraunhofer constate en ce sens :

> « les algorithmes sont mieux adaptés aux visages caucasiens. Cependant, il existe également des caractéristiques physionomiques des différents groupes ethniques qui empêchent leur reconnaissance, même s'ils étaient mieux formés. Il restera donc difficile d'y parvenir avec la technologie existante »[147].

Cet avis est partagé par Florian Gallwitz, expert en reconnaissance faciale de l'Institut de Technologie de Nuremberg qui s'est exprimé sur ces derniers et déplorait considérer la 1re phase de test comme un échec cuisant. La faute au dispositif qui était lui-même loin d'être au point (des caméras aux angles rendaient compliqué la reconnaissance des visages, certaines étaient placées face à la lumière).

Pour autant, le ministre de l'intérieur fait part la volonté d'optimiser et augmenter les taux de réussites de manière à réduire les faux positifs en dessous de la barre des 0,1% jusqu'à 0,00018% en combinant différents systèmes et opérateurs[148]. Il envisage en outre une large diffusion du dispositif à l'avenir :

> « Les résultats montrent que la technologie de reconnaissance faciale peut apporter un soutien considérable à nos policiers dans leur vie quotidienne. Les systèmes ont fait leurs preuves de manière impressionnante, de sorte qu'une large introduction est possible. Nous pouvons les utiliser pour rendre le travail de la police encore plus efficace dans certains domaines, améliorant ainsi la sécurité des citoyens »[149].

Dans le cadre de la nouvelle loi sur la police fédérale, le ministre projetait d'élargir le recours à la reconnaissance faciale dans le cadre de la détention préventive, pour empêcher les supporters de football violents ou les djihadistes de quitter le pays. Il est toutefois revenu lors du vote des amendements. Dans le cadre de l'adoption de cette loi, les préconisations du Commissaire fédéral à la protection des données et celles des défenseurs des droits ont primé.

---

145 « *Biometrische Gesichtserkennung* »,
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Biometrie/Gesichtserkennung_pdf.pdf?__blob=publicationFile&v=1

146 Interview de F. KIRCHBUCHNER de l'Institut Fraunhofer-Gesellschaft par Christiane KNOLL, le 13 janvier 2020 pour le média *Deutschlandfunk*.
https://www.deutschlandfunk.de/automatische-gesichtserkennung-es-ist-moeglich-die-systeme.676.de.html?dram:article_id=468082

147 « *Es liegt zum einen, wie Sie schon gesagt haben, daran, dass die Algorithmen besser auf kaukasische Gesichter trainiert sind. Allerdings gibt es auch physiognomische Eigenschaften unterschiedlicher Ethnien, die eine Erkennung, selbst wenn man sie besser trainieren würde, verhindern. Also hier wird es schwierig bleiben mit der vorhandenen Technik* », *Ibidem*.

148 « *Das bedeutet, dass bei 1000 Abgleichen auf einem Bahnhof lediglich ein einziger Abgleich durch das System fehlerhaft erkannt wird. Dieser Wert lässt sich aber durch Kombination verschiedener Systeme technisch auf bis zu 0,00018% und damit auf ein verschwindend geringes Maß reduzieren. Die Systeme haben sich damit für einen Einsatz im Polizeialltag bewährt.* »
https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2018/10/gesichtserkennung-suedkreuz.html

149 Ministère fédéral de l'Intérieur, Communiqué de presse du 11 octobre 2018 « *Projet de reconnaissance faciale réussi – Publication des résultats des tests* ». https://www.bundespolizei.de/Web/DE/04Aktuelles/01Meldungen/2018/10/181011_abschlussbericht_gesichtserkennung_pm_down.pdf;jsessionid=201E95629322BD206B6E40FC62A10C27.1_cid289?__blob=publicationFile&v=1

BIBLIOGRAPHIE

I. Législation

- Loi fédérale sur la protection des données (BDSG) du 30 juin 2017, modifiée par l'article 12 de la loi du 20 novembre 2019.
  https://www.gesetze-im-internet.de/bdsg_2018/BJNR209710017.html
- Deuxième loi d'adaptation de la loi sur la protection des données au règlement (UE) 2016/679 et de transposition de la directive (UE) 2016/680.
  http://dipbt.bundestag.de/extrakt/ba/WP19/2390/239070.html
  https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/1983/12/rs19831215_1bvr020983.html
- Article 2, Loi fondamentale de la République fédérale d'Allemagne (*Grundgesetz für die Bundesrepublik Deutschland*).
  https://www.gesetze-im-internet.de/gg/art_2.html

II. Prise de position des autorités instances fédérales

- Commissaire fédéral à la protection des données et au droit à l'information « *Un délégué fédéral à la protection des données met en garde contre la reconnaissance faciale* », 24 janvier 2019. « *Bundesdatenschutzbeauftragter mahnt Zurückhaltung bei Gesichtserkennung an* ».
  https://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2019/02_Zur%C3%BCckhaltungbeiGesichtserkennung.html
- Daten Ethik Kommission, "*Opinion of the Data Ethics Commission*", 10 octobre 2019. https://www.bmjv.de/SharedDocs/Downloads/DE/Themen/Fokusthemen/Gutachten_DEK_EN_lang.pdf?__blob=publicationFile&v=3
- Direction générale de la police fédérale, « *Reconnaisance biométrique du visage* » (*Biometrische Gesichtserkennung*) dans le cadre de tests des systèmes d'analyse vidéo intelligents par le ministère fédéral de l'intérieur, le siège de la police fédérale, l'Office fédéral de la police criminelle et la Deutsche Bahn AG à la gare de Berlin Südkreuz [en ligne], 18 septembre 2018, [consulté le 16/01/2020]. https://cutt.ly/RrYnZOx
- Ministère fédéral de l'Intérieur, Communiqué de presse du 11 octobre 2018 « *Projet de reconnaissance faciale réussi – Publication des résultats des tests* ».
  https://www.bundespolizei.de/Web/DE/04Aktuelles/01Meldungen/2018/10/181011_abschlussbericht_gesichtserkennung_pm_down.pdf;jsessionid=201E95629322BD206B6E40FC62A10C27.1_cid289?__blob=publicationFile&v=1

III. Jurisprudence

- Arrêt rendu par la Cour constitutionnelle de Karlsruhe le 15 décembre 1983 consacrant un droit à « l'autodétermination informationnelle », attaché à la personne et visant à garantir la capacité d'un individu à décider de la communication et de l'utilisation de ses données à caractère personnel.

IV. Presse numérique

- U. Kelber, « Le responsable de la protection des données met en garde contre la reconnaissance automatique des visages », [en ligne], *t3n*, 16 janvier 2019, [consulté le 16/01/2020], https://t3n.de/news/datenschutzbeauftragter-kelber-1137512/
- Interview de f. kirchbuchner de l'Institut *Fraunhofer-Gesellschaft* par Christiane knoll, le 13 janvier 2020 pour le média *Deutschlandfunk*.
  https://www.deutschlandfunk.de/automatische-gesichtserkennung-es-ist-moeglich-die-systeme.676.de.html?dram:article_id=468082

Belgique

I. Législation

S'il n'existe pas de cadre légal spécifique à la reconnaissance faciale en Belgique, les législations relatives à la protection des données (A), à la vidéosurveillance (B) et à la fonction de police (C) posent les premiers jalons d'un encadrement légal de la technologie.

A - La loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel

La **loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel**[150] abroge définitivement la loi sur la vie privée du 8 décembre 1992 et poursuit la mise en œuvre de certains aspects du RGPD.

Le traitement des données biométriques fait l'objet d'une protection particulière, notamment mentionné aux articles 9, 34 et 76 de la loi :

- L'**article 9** impose au responsable de traitement de prendre des mesures supplémentaires en matière d'accès aux données génétiques, biométriques ou concernant la santé : 1° les catégories de personnes ayant accès aux données à caractère personnel, sont désignées par le responsable du traitement ou, le cas échéant, par le sous-traitant, avec une description précise de leur fonction par rapport au traitement des données visées;
  2° la liste des catégories des personnes ainsi désignées est tenue à la disposition de l'autorité de contrôle compétente par le responsable du traitement ou, le cas échéant, par le sous-traitant;
  3° il veille à ce que les personnes désignées soient tenues, par une obligation légale ou statutaire, ou par une disposition contractuelle équivalente, au respect du caractère confidentiel des données visées.
- L'**article 34** retranscrit l'article 9 du RGPD, en posant une interdiction de principe de traiter des données personnelles à caractère sensible, sauf exception.
- L'**article 76** émet une exception à cette interdiction de principe : dans l'intérêt de l'exercice de leurs missions, les services de renseignement et de sécurité peuvent traiter des données à caractère personnel de toute nature, y compris des données génétiques et biométriques, ce qui semble laisser une porte d'entrée à l'usage de la reconnaissance faciale par ces services.

B - La loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance

La **loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance** (dite « loi caméras ») [151], modifiée par les lois du 4 avril 2014, du 2 octobre 2017 et du 21 mars 2018, ne prévoit pas la possibilité de recourir à des caméras avec reconnaissance faciale sur l'espace public. En effet, le texte autorise l'utilisation de caméras de surveillance mobiles ou fixes dites « intelligentes » (comprenant des logiciels qui, couplés à des registres ou des fichiers, peuvent traiter les images de manière autonome) uniquement pour la reconnaissance des plaques d'immatriculation (« caméras ANPR »). L'introduction de dispositifs de reconnaissance faciale dans l'espace public supposerait donc une modification de la loi caméras ou l'adoption d'une nouvelle loi.

---

150 Loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, 30 juillet 2018
http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2018073046&table_name=loi

151 Loi réglant l'installation et l'utilisation de caméras de surveillance., 21 mars 2007.http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2007032139&table_name=loi

L'utilisation de caméras par la police - à savoir toutes les caméras utilisées par les services de police – constitue un cas spécifique qui relève de la loi sur la fonction de police du 5 août 1992.

C - La loi du 5 août 1992 sur la fonction de police

La **loi du 5 août 1992 sur la fonction de police**[152] autorise, en son article 44/1 §2., le traitement de données biométriques « dans le but d'assurer l'identification certaine de la personne concernée visée à l'article 44/5, § 1er, 2° à 7°[153] et § 3 1° à 6°[154]. Les données biométriques des personnes visées au § 3, 7° à 9°[155], et au § 4[156] de l'article 44/5 sont traitées uniquement sur la base du consentement de la personne concernée ou lorsqu'elles sont manifestement rendues publiques par la personne concernée ou encore pour sauvegarder les intérêts vitaux de la personne concernée ou d'une autre personne physique. Lorsque le traitement des données biométriques en vue de l'identification unique des personnes concernées, en particulier par le recours aux nouvelles technologies, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées, le responsable du traitement ou son sous-traitant consulte l'Organe de contrôle; ». La loi sur la fonction de police ne pose donc pas d'interdiction s'agissant du traitement des données biométriques de personnes recherchées par les forces de police ; l'article précité pourrait même en constituer le fondement. Dans cette hypothèse, l'Organe de contrôle de l'information policière serait l'autorité compétente pour en accompagner la mise en place.

A ce jour, rappelons toutefois que la loi prévoit exclusivement le recours aux caméras intelligentes, fixes ou mobiles, en matière de reconnaissance automatique des plaques d'immatriculation. Pour permettre le recours à cette technologie, le texte autorise la création d'une « banque de données techniques » spécifique tant au niveau local qu'au niveau national.

En conséquence, la législation belge est ambiguë : si la loi peut être interprétée comme autorisant la police à recourir à la technologie dans l'espace public, elle n'autorise pas, pour autant, la création d'une base de données spécifique à cet effet. Ce texte nécessite donc une adaptation pour permettre l'usage, par les forces de police, de la reconnaissance faciale comme moyen d'identification dans l'espace public. Cette réforme pourrait s'inspirer des dispositions spécifiques à l'usage de caméras intelligentes en matière de reconnaissance automatique des plaques d'immatriculation, tout en tenant compte des enjeux spécifiques liés à l'usage de la sensibilité des données biométriques.

A contrario, il est possible d'interpréter ce texte comme autorisant l'utilisation d'un dispositif de reconnais-

152 Loi sur la fonction de police, 5 août 1992http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=1992080552&table_name=loi

153 2° les données relatives aux personnes impliquées dans les phénomènes de police administrative entendus comme, l›ensemble des problèmes, portant atteinte à l›ordre public et nécessitant des mesures appropriées de police administrative, parce qu›ils sont de même nature et répétitifs, qu›ils sont commis par les mêmes personnes ou qu›ils visent les mêmes catégories de victimes ou de lieux;
3° les données relatives aux membres d'un groupement national ou international susceptible de porter atteinte à l'ordre public tel que visé à l'article 14;
4° les données relatives aux personnes susceptibles de porter atteinte aux personnes ou aux biens mobiliers et immobiliers à protéger et les données relatives aux personnes qui peuvent en être la cible;
5° les données relatives aux personnes visées aux articles 18 à 21;
6° les données relatives aux personnes enregistrées en police judiciaire pour un fait infractionnel commis dans le cadre du maintien de l'ordre public;
7° les données relatives aux personnes faisant l'objet d'une mesure administrative prise par une autorité administrative compétente et que les services de police sont chargés de suivre par ou en vertu de la loi, du décret ou de l'ordonnance.

154 1° les données relatives aux suspects d›un fait pénal et aux personnes condamnées;
2° les données relatives aux auteurs et suspects d'une infraction sanctionnée administrativement et constatée par la police;
3° les données relatives aux personnes décédées de manière suspecte;
4° les données relatives aux personnes disparues;
5° les données relatives aux personnes évadées ou qui ont tenté de s'évader;
6° les données relatives à l'exécution des peines et à ses modalités d'exécution;

155 7° les données relatives aux témoins d›un fait pénal;
8° les données relatives aux personnes visées aux articles 47novies/1, § 1er, 47decies, § 1er, et 102, 1° à 3°, du Code d'instruction criminelle;
9° les données relatives aux victimes d'un fait pénal.

156 1° les données relatives aux personnes qui se sont constituées partie civile ou aux personnes lésées;
2° les données relatives aux personnes civilement responsables d'un fait pénal.

sance faciale qui n'est pas relié à une base de données. Partant de là, l'usage de la reconnaissance faciale comme moyen d'authentification serait légalement possible pour les forces de police, contrairement à l'usage de la reconnaissance faciale comme moyen d'identification qui implique nécessairement la constitution, même temporaire, d'une base de données reliée au dispositif.

De manière générale, notons que la police belge se montre proactive dans l'usage des nouvelles technologies. En 2018 déjà, sur le modèle des caméras corporelles introduites aux Pays-Bas[157], la police avait souhaité expérimenter localement ce dispositif. Pour cela, elle avait réussi à obtenir une adaptation du cadre légal permettant, aujourd'hui, de généraliser ce dispositif à l'ensemble du pays[158]. La question de savoir si le législateur belge franchira le pas de la modification législative pour favoriser le recours aux technologies de reconnaissance faciale par la police se pose donc légitimement.

II. Position de l'autorité de protection des données

Au regard des débats européen, l'Autorité de protection des données personnelles belge s'est positionnée très tôt : dès 2008 celle-ci a pris position sur l'utilisation de la reconnaissance faciale comme ***moyen d'authentification*** biométrique **(A)**. Toutefois, l'utilisation de la reconnaissance faciale comme ***moyen d'identification*** n'a pas fait l'objet d'un avis ; seules des prises de position, sporadiques, permettent d'identifier sa position **(B)**.

A - La reconnaissance faciale comme moyen d'authentification biométrique

L'Autorité de protection des données personnelles a rendu un **avis n°17/2008 en date du 9 avril 2008**[159] sur le traitement de données biométriques dans le cadre de l'authentification de personnes[160]. Précisions que cet avis ne porte pas sur l'utilisation de la biométrie afin de procéder au contrôle des frontières, ni aux traitements effectués par les services de police et services de sécurité, ces hypothèses ne relevant pas de sa compétence.

Dès 2008, l'autorité de contrôle semblait hostile à la généralisation du recours à l'authentification biométrique : « de manière générale, il convient d'être conscient du choix de société que constitue une généralisation du recours à la biométrie, et des risques de désensibilisation du public que cela comporte. La biométrie, moyen d'authentification fort, ne devrait être utilisée que parce qu'elle constitue le seul moyen pour réaliser le but recherché, et pas seulement parce qu'elle est pratique, ou parce qu'elle «fait moderne» »[161].

Si elle reconnaissait la forte fiabilité, sur le principe, des technologies biométriques, elle émettait toutefois une réserve importante sur l'utilité de leur déploiement au regard des taux d'erreur. Elle exigeait alors que les systèmes mis en place aient un taux de faux rejets « le plus bas possible »[162], tout en assurant un juste équilibre avec le taux de fausses acceptations[163].

Dans ce même avis, l'autorité de contrôle belge rappelait, par ailleurs, l'applicabilité de la loi relative aux traitements de données et de ses grands principes, l'utilisation de la biométrie impliquant un traitement de données sensibles.

---

157 Voy. la partie consacrée aux Pays-Bas.

158 « La caméra doit être visible pour le citoyen. Celle-ci n'enregistre que si un bouton-poussoir est activé. Le cadre légal est strict : le policier doit signaler lorsqu'il active la vidéo. Le citoyen n'a pas le pouvoir de s'y opposer. », L. Van de Berg, « Madame, Monsieur, vous êtes filmés !»: quelles règles encadrent les bodycams de la police ? » [en ligne], *RTBF*, 14 janvier 2020, [consulté le 23/03/2020], https://www.rtbf.be/info/societe/detail_madame-monsieur-vous-etes-filme-quelles-regles-encadrent-les-bodycams-de-la-police?id=10407167)

159 Commission de la protection de la vie privee, Avis d'initiative n°17/2008 du 9 avril 2008 relatif aux traitements de données biométriques dans le cadre de l'authentification des personnes, https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/avis_17_2008_0.pdf

160 Définie ici comme « *un processus qui consiste à vérifier l'identité prétendue d'une entité donnée (telle une personne)* »

161 Autorité de la protection des données, *Un choix de société*, https://www.autoriteprotectiondonnees.be/un-choix-de-soci%C3%A9t%C3%A9

162 Rejet d'un certain pourcentage de personnes qui auraient dû être acceptées

163 Acceptation d'un certain pourcentage de personnes qui n'auraient pas dû l'être.

S'agissant de la légitimité d'un tel traitement, le traitement des données biométriques à des fins d'authentification de personnes peut en principe, selon l'autorité, intervenir lorsque les personnes concernées ont donné leur consentement de façon libre, spécifique et informée. L'autorité remarque toutefois que le consentement présente cependant des limites. Le recours à la technologie peut également être autorisé s'il est prévu par une loi, ou si le responsable de traitement fait valoir un intérêt légitime prépondérant prévalant l'intérêt ou les droits et libertés fondamentaux de la personne concernée.

S'agissant du principe de proportionnalité, l'autorité rappelle que l'intérêt général ou les intérêts légitimes du responsable de traitement doivent être mis en balance avec le droit à la protection de la vie privée des personnes enregistrées. Pour le responsable de traitement, outre les avantages relatifs aux coûts et à la facilité du système, l'avantage spécifique de l'utilisation d'un système biométrique est l'amélioration de la sécurité dans de nombreux cas. La Commission sur la protection de la vie privée – ancien nom de l'Autorité de protection des données personnelles au moment de l'avis – contrebalance toutefois cet argument en soulignant le fait que l'utilisation de données biométriques suscite des considérations particulières relatives à la protection des données, de la vie privée et de la dignité humaine. Par conséquent, l'appréciation de la proportionnalité des traitements de données biométriques doit être réalisée par les responsables de traitement de manière stricte : la biométrie est un moyen d'authentification fort, et il devrait être réservé aux situations nécessitant un tel niveau de sécurité. Par exemple, la Commission met en doute la nécessité et proportionnalité d'utiliser un système biométrique de manière généralisée dans le cadre scolaire. Il en est de même pour la gestion des horaires des salariés.

Pour savoir si un système biométrique est proportionné, la Commission donne quelques recommandations en la matière :

- Ne pas utiliser des systèmes biométriques stockant les données biométriques de référence dans une bonne de donnée
- Ne pas stocker les données biométriques brutes (images), mais plutôt les gabarits, c'est-à-dire les données pertinentes extraites des données biométriques brutes
- Ne pas utiliser des technologies qui permettent de collecter et/ou de traiter des données biométriques à l'insu de la personne concernée
- Utiliser un système biométrique sécurisé

S'agissant de l'information de la personne concernée, l'autorité de contrôle précise que cette information inclut les finalités du traitement, l'identité du responsable de traitement et des destinataires des données ainsi que l'existence du droit d'accès et de rectification de la personne concernée.

Afin de garantir une transparence vis-à-vis des personnes concernées, il convient également de fournir spontanément de l'information quant :

- au type de système biométrique utilisé (type de stockage notamment) ;
- à l'existence d'un taux d'erreur de reconnaissance inhérent à tout système biométrique ;
- à la procédure à suivre par la personne concernée lors d'une prétendue non-reconnaissance par le système, afin d'éviter que les systèmes biométriques ne soient présentés comme étant des systèmes infaillibles.

S'agissant de la durée de stockage des données, la Commission souligne que celle-ci ne doit pas aller au-delà de la durée nécessaire pour la réalisation de la finalité poursuivie. À ce titre, le capteur biométrique qui permet de collecter la caractéristique biométrique ne doit pas conserver de copie de la donnée biométrique au-delà de la durée nécessaire pour effectuer la comparaison.

S'agissant, enfin, des mesures techniques et organisationnelles de sécurité, le niveau de sécurité doit être particulièrement élevé compte tenu de la nature particulière des données biométriques et des risques d'atteintes à la sécurité des données.

Ainsi, l'Autorité de protection des données personnelles belge, dès 2008, avait identifié la nécessité

de légiférer non seulement pour encadrer strictement le déploiement de la reconnaissance faciale comme moyen d'authentification - et ainsi respecter les principes de nécessité et de proportionnalité -, mais également pour en assurer la légitimité. À défaut de législation, cet avis rappelle l'ensemble des grands principes de la protection des données personnelles devant être pris en compte lors de la mise en place d'un tel dispositif.

B - La reconnaissance faciale comme moyen d'identification

Si l'Autorité de protection des données personnelles affirmait dès 2008 qu'elle se prononcerait sur l'utilisation de la reconnaissance faciale comme moyen d'identification en temps voulu, elle ne l'a jamais fait. La seule prise de position sur cette question procède d'une décision de 2019. Cette décision concerne le caractère obligatoire de l'analyse d'impact pour les traitements de données biométriques en vue de l'identification unique des personnes **(1)**. En l'absence d'une réelle prise de position, et malgré la volonté manifestée en pratique de recourir à cette technologie, l'Organe de contrôle de l'information policière s'est fermement opposé au projet mené par la police fédérale **(2)**.

1. L'obligation d'une analyse d'impact pour les traitements de données biométriques en vue de l'identification unique des personnes

Dans une **décision n°01/2019 du 6 janvier 2019**[164], le Secrétariat général de l'Autorité de protection des données a adopté une liste des catégories de traitement devant faire l'objet d'une analyse d'impact relative à la protection des données conformément à l'**article 35.4 du RGPD**.

Il est intéressant de remarquer que les traitements qui utilisent des données biométriques, en vue de l'identification unique des personnes concernées se trouvant dans un lieu public ou dans un lieu privé accessible au public, sont les premiers à être cités. Cette mention témoigne du risque particulier d'atteinte aux droits et libertés des personnes que constitue ces dispositifs comme moyen d'identification pour l'Autorité. Il apparaît donc indispensable de réaliser une analyse d'impact et de consulter l'Autorité de protection des données préalablement au déploiement de cette technologie.

Il est *a contrario* surprenant que les traitements qui utilisent des données biométriques en vue de l'authentification des personnes ne soient pas mentionnés dans cette liste.

2. La prise de position de l'Organe de contrôle de l'information policière

En septembre 2019, le commissaire général de la police fédérale a manifesté la volonté d'équiper les agents de police de l'aéroport de Bruxelles d'un dispositif de reconnaissance faciale d'identification[165]. En réponse, l'Organe de contrôle de l'information policière a indiqué que, contrairement à la vidéosurveillance, le recours à la reconnaissance faciale par les forces de police n'est pas légal en Belgique[166].

L'Organe de contrôle de l'information policière, tenu au secret professionnel, n'a pu divulguer le détail de son évaluation du projet[167]. Bien qu'il n'ait pas rendu d'avis officiel[168], sa position a été relayée par la presse belge.

164 Secrétariat général de l'Autorité de protection des données, *Adoption de la liste des catégories de traitement devant faire l'objet d'une analyse d'impact relative à la protection des données conformément à l'article 35.4 du Règlement général sur la Protection des données* (CO-A-2018-001) , n°01/2019, 16 janvier 2019, https://www.autoriteprotectiondonnees.be/sites/privacy-commission/files/documents/01_2019_SG.pdf

165 Voy. *Infra*.

166 T. Blancmont, « Aéroport de Bruxelles : reconnaissance faciale et Dashboard » [en ligne], *Air journal*, 11 juillet 2019, [consulté le 14/01/2019], https://www.air-journal.fr/2019-07-11-aeroport-de-bruxelles-reconnaissance-faciale-et-dashboard-5213706.html

167 Ds Avond, "Federale politie moet gezichtsherkenning stopzetten" [en ligne], *De Standaard*, 20 septembre 2019, [consulté le 11/03/2020], https://www.standaard.be/cnt/dmf20190920_04618911?articlehash=78C468B42191245F2A8AF844715B8EC50284A320C-D3B402C88EB743AE296BC05D9815613E26EEF112EB4A61FF7E4A0E0769D77397538564A75018A2BF311E6DE

168 Contrairement aux avis concernant tous les projets de réglementation présentant un lien avec les compétences de l'autorité publiés sur son site (https://www.organedecontrole.be/publications/avis-r%C3%A9glementation),les avis et recommandations à l'égard des citoyens, des professionnels et des autorités ne font pas l'objet de publication (https://www.organe-decontrole.be/publications/avis-recommandations)

Cette autorité de contrôle n'aurait pas été informée, en amont, par la police, laquelle ne l'a pas sollicitée pour évaluer l'impact du dispositif sur la vie privée, en méconnaissance de la loi du 5 août 1992 sur la fonction de police.

La police fédérale souhaitait, en outre, constituer une base de données temporaire avec les gabarits de visages – c'est-à-dire les empreintes biométriques – des voyageurs[169], ce qui constitue une seconde violation de la loi précitée. Rappelons que la loi de 1992 autorise le seul le stockage de données provenant de système de reconnaissance de plaques d'immatriculation.

III. Cas d'usage

La reconnaissance faciale a d'abord été expérimentée à l'aéroport Bruxelles-National comme moyen d'authentification des passagers, puis moyen d'identification **(A)**. Le stade du club de football de Molenbeek a également expérimenté la reconnaissance faciale comme moyen d'authentification pour faciliter l'accès au stade des supporters abonnés **(B)**.

A - Reconnaissance faciale d'authentification et d'identification dans l'aéroport Bruxelles-National

Depuis 2015, six postes de contrôle frontalier automatisés ont été installés à l'aéroport Brussels-National, afin d'authentifier l'identité des citoyens de l'Union européenne, âgés d'au moins 12 ans et provenant d'un pays situé en dehors de l'espace Schengen.

L'« *e-gate* » compare la photo du document d'identité (carte d'identité ou passeport) à une photo numérique prise sur place. Ce système informatique contrôle, par ailleurs, l'authenticité du document d'identité et vérifie également si le titulaire du document d'identité est signalé « à rechercher » dans la banque de données de la police[170].Ce dispositif étant antérieur au RGPD, il n'a pas fait l'objet d'une analyse d'impact relative à la protection des données imposée depuis le 25 mai 2018.

Cinq ans après leur installation, l'aéroport de Bruxelles a finalement supprimé le dispositif, les portes électroniques ayant recours à la reconnaissance faciale s'étant révélées « constamment défaillantes »[171]. Elles avaient ainsi permis à une passagère de passer alors qu'elle avait scanné le passeport de son mari[172]. Ces portes devraient être remplacées par un autre « système plus efficace », mais aucune précision n'a été donnée sur la solution alternative qui serait utilisée. Une procédure d'appels d'offres est en cours. La police fédérale a manifesté la volonté d'uniformiser les dispositifs à l'échelle européenne, afin d'avoir un système uniforme de sécurisation des aéroports, gares, etc.[173]

Cette expérience a donc mis en évidence les lacunes encore nombreuses de la technologie de reconnaissance faciale, alors même que l'investissement dans ce dispositif avait été conséquent : en effet, le dispositif avait coûté 2,4 millions d'euros, en grande partie financé (à hauteur de 75%) par le Fonds européen pour les frontières extérieures[174].

Par ailleurs, en septembre 2019, le commissaire général de la police fédérale a annoncé son intention d'équiper toutes les caméras de l'aéroport Bruxelles-National (aéroport de Zaventem) d'un logiciel de

169 Ds Avond, "Federale politie moet gezichtsherkenning stopzetten", précédemment cité.

170 L'Echo, « La reconnaissance faciale arrive à Brussels Airport » [en ligne], *L'Echo*, 10 juillet 2015, [consulté le 13/01/2020], https://www.lecho.be/economie-politique/belgique-bruxelles/La-reconnaissance-faciale-arrive-a-Brussels-Airport/9654127?utm_medium=twitter&utm_source=twitterfeed

171 S. Barik, "Brussels Airport to scrap facial recognition enabled e-gates as the system was 'constantly defective': Report" [en ligne], *Medianama*, 18 février 2020, [consulté le 25/02/2020], https://www.medianama.com/2020/02/223-brussels-airport-facial-recognition-egates-scrapped/

172 *Ibidem.*

173 A. François, « Les coûteux portiques de sécurité à Brussels Airport doivent déjà être remplacés » [en ligne], *Vrt*, 14 février 2020, [consulté le 25/02/2020], https://www.vrt.be/vrtnws/fr/2020/02/14/les-couteux-portiques-de-securite-a-brussels-airport-doivent-dej/

174 Belga, « Brussels Airport : contrôle automatisé pour les passeports européens » [en ligne], *Rtbf.be*, 10 juillet 2015, [consulté le 26/02/2020], https://www.rtbf.be/info/belgique/detail_brussels-airport-controle-automatise-pour-les-passeports-europeens?id=9029301

reconnaissance faciale. L'objectif de ce réseau de caméras relié au logiciel vise à permettre aux agents de police présents à l'aéroport d'identifier des suspects en matière de terrorisme et de criminalité organisée, sur place et en temps réel. Le commissaire général de la police fédérale, Marc de Mesmaeker, a annoncé avoir un accord avec l'exploitant et les syndicats » pour la mise en place d'un tel dispositif. Aucun acteur n'a pour le moment été communiqué pour l'heure.

Toutefois, l'Organe de contrôle de l'information policière a ordonné que le projet soit provisoirement abandonné, n'ayant pas été informé de l'expérimentation ni sollicité pour une analyse d'impact relative à la protection des données. Comme évoqué dans les développements précédents (II.B-2), l'instance a établi que le projet contrevenait à la loi sur la fonction de police et celle sur la protection des données.

Prenant acte de cette prise de position, la police fédérale a réitéré sa volonté de recourir à la technologie, tout en s'engageant à le faire dans le respect des droits de l'Homme et des libertés fondamentales. Elle prévoit ainsi de consulter les autorités politiques, le Comité permanent de la police locale ainsi que l'autorité de contrôle[175].

B - Reconnaissance faciale d'authentification au stade R.W.D. Molenbeek

Au premier trimestre de l'année 2019, le stade du club de football belge *Racing White Daring Molenbeek* (ou RWDM) a initié, pour un an, une expérimentation de la technologie de reconnaissance faciale permettant aux supporters du club, titulaires d'un abonnement saisonnier, d'entrer plus facilement dans le stade par le biais d'une « *fast lane* » (file prioritaire).

Cette expérimentation est légitimée sur la base du consentement des participants, puisque seuls les supporters qui ont donné leur accord auront leur visage authentifié : environ 500, soit un quart du total des abonnés. Il s'agit de ceux qui ont acheté leur abonnement pour la saison 2018-2019 via le site internet du club, qui ont alors accepté de donner leur accord pour participer au projet et qui ont fourni leur photo sur le site.

La confidentialité des données est garantie par des mesures techniques : les photos scannées et visages associés aux noms des supporters sont uniquement stockés sur un serveur interne au RWDM, non relié à Internet ni aucun autre système et seul le personnel autorisé du RWDM peut y avoir accès. Ces données ne sont donc pas transmises à des tiers ou croisées avec d'autres bases de données.

Le supporter peut à tout moment retirer son consentement et décider de quitter l'expérience par une demande en ligne. À défaut de réabonnement, ses données sont effacées au bout d'un mois.

Le service a été mis en place par la société Zetes et utilise la technologie de reconnaissance faciale de Panasonic. Il est important de noter que, depuis juillet 2017, le groupe japonais Panasonic a pris le contrôle de la société belge Zetes à 100 %. L'objectif de l'entreprise nippone est, à terme, de pouvoir prouver l'efficacité de son système et de le vendre à d'autres structures, comme les festivals de musique par exemple, les aéroports ou les autres rassemblements de foule[176].

L'existence d'une analyse d'impact n'a été diffusée et l'Autorité de protection des données personnelles n'a pas manifesté publiquement une quelconque prise de position sur ce cas d'usage. Par ailleurs, aucun bilan de cette expérimentation n'a à ce jour été communiqué. Un manque de transparence est ici à souligner.

175 Ds Avond, précédemment cité.

176 B. Schmitz, « Le RWDM comme laboratoire pour une technologie de reconnaissance faciale » [en ligne], *RTBF*, 5 septembre 2018, [consulté le 14/01/2020], https://www.rtbf.be/info/regions/bruxelles/detail_le-rwdm-comme-laboratoire-pour-une-technologie-de-reconnaissance-faciale?id=10011249

BIBLIOGRAPHIE

I. Législation

- Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2007032139&table_name=loi
- Loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance, http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2007032139&table_name=loi
- Loi du 5 août 1992 sur la fonction de police, http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=1992080552&table_name=loi

II. Prise de position des autorités régulatrices de la protection des données

- Autorité de la protection des données, « Un choix de société », https://www.autoriteprotectiondonnees.be/un-choix-de-soci%C3%A9t%C3%A9
- Commission de la protection de la vie privée, avis d'initiative n°17/2008 du 9 avril 2008 relatif aux traitements de données biométriques dans le cadre de l'authentification des personnes, https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/avis_17_2008_0.pdf
- Secrétariat général de l'Autorité de protection des données, « Adoption de la liste des catégories de traitement devant faire l'objet d'une analyse d'impact relative à la protection des données conformément à l'article 35.4 du Règlement général sur la Protection des données (CO-A-2018-001) », n°01/2019, 16 janvier 2019, https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/01_2019_SG.pdf

III. Presse numérique

- Avond Ds, "Federale politie moet gezichtsherkenning stopzetten" [en ligne], *De Standaard*, 20 septembre 2019, [consulté le 11/03/2020], https://www.standaard.be/cnt/dmf20190920_04618911?articlehash=78C468B42191245F2A8AF-844715B8EC50284A320CD3B402C88EB743AE296BC05D9815613E26EEF112EB4A61FF7E4A0E-0769D77397538564A75018A2BF311E6DE
- Barik S., "Brussels Airport to scrap facial recognition enabled e-gates as the system was 'constantly defective': Report" [en ligne], *Medianama*, 18 février 2020, [consulté le 25/02/2020], https://www.medianama.com/2020/02/223-brussels-airport-facial-recognition-egates-scrapped/
- Belga, « Brussels Airport : contrôle automatisé pour les passeports européens » [en ligne], *Rtbf.be*, 10 juillet 2015, [consulté le 26/02/2020], https://www.rtbf.be/info/belgique/detail_brussels-airport-controle-automatise-pour-les-passeports-europeens?id=9029301
- Blancmont T., « Aéroport de Bruxelles : reconnaissance faciale et Dashboard » [en ligne], *Air journal*, 11 juillet 2019, [consulté le 14/01/2019], https://www.air-journal.fr/2019-07-11-aeroport-de-bruxelles-reconnaissance-faciale-et-dashboard-5213706.html
- François A., « Les coûteux portiques de sécurité à Brussels Airport doivent déjà être remplacés » [en ligne], *Vrt*, 14 février 2020, [consulté le 25/02/2020],

https://www.vrt.be/vrtnws/fr/2020/02/14/les-couteux-portiques-de-securite-a-brussels-airport-doivent-dej/

- L'Echo, « La reconnaissance faciale arrive à Brussels Airport », *L'Echo*, 10 juillet 2015, [consulté le 13/01/2020], https://www.lecho.be/economie-politique/belgique-bruxelles/La-reconnaissance-faciale-arrive-a-Brussels-Airport/9654127?utm_medium=twitter&utm_source=twitterfeed
- Schmitz B., « Le RWDM comme laboratoire pour une technologie de reconnaissance faciale » [en ligne], *RTBF*, 5 septembre 2018, [consulté le 14/01/2020], https://www.rtbf.be/info/regions/bruxelles/detail_le-rwdm-comme-laboratoire-pour-une-technologie-de-reconnaissance-faciale?id=10011249
- Van de Berg L., « Madame, Monsieur, vous êtes filmés !»: quelles règles encadrent les bodycams de la police ? » [en ligne], *RTBF*, 14 janvier 2020, [consulté le 23/03/2020], https://www.rtbf.be/info/societe/detail_madame-monsieur-vous-etes-filme-quelles-regles-encadrent-les-bodycams-de-la-police?id=10407167

Espagne

I. Législation

Les données à caractère personnel en Espagne sont protégées par la loi organique n°3/2018 du 5 décembre 2018 relative à la protection des données à caractère personnel et à la garantie des droits numériques [177]. Elle est la loi d'application du RGPD[178].

Concernant plus spécifiquement la reconnaissance faciale, aucun texte spécifique n'existe pour le moment. Seuls des orientations et guides pratiques rédigés par l'*Agencia Española de Protección de Datos* (AEPD) font référence.

II. Position de l'autorité de contrôle

L'AEPD s'est prononcée, dans un guide pratique, sur l'application de l'article 35.1 du RGPD relatif à la ***nécessité d'effectuer une analyse de l'impact*** des opérations de traitement envisagées sur la protection des données à caractère personnel[179].

L'Autorité de contrôle espagnole identifie plusieurs cas d'activités susceptibles d'engendrer une analyse d'impact[180]. Il en va ainsi de la combinaison des empreintes digitales et de la reconnaissance faciale pour améliorer le contrôle de l'accès physique.

En mars 2018, dans une seconde orientation[181], l'AEPD s'est positionnée ***sur l'utilisation de la reconnaissance faciale dans les établissements scolaires***. Elle précise que le consentement exprès des étudiants de plus de quatorze ans - ou celui des parents ou tuteurs dans le cas où ils ont moins de quatorze ans – est requis[182].

L'Autorité de contrôle espagnole indique également que la capture d'images dans des environnements à forte fréquentation par les enfants tels que les écoles, les jardins d'enfants, les centres de loisirs nécessite certaines précautions. Ainsi, l'installation de caméras de vidéosurveillance dans ces environnements afin de contrôler les comportements susceptibles d'affecter la sécurité doit être proportionnelle à la finalité poursuivie, et ne se substituer en aucun cas aux missions de surveillance[183]. Aussi, les caméras peuvent être installées dès lors qu'elles répondent à la protection de l'intérêt supérieur de l'enfant, lorsque l'intégrité physique, psychologique et émotionnelle est potentiellement en danger. La zone soumise à la vidéosurveillance doit

177 Loi organique n°3/2018 du 5 décembre 2018, https://www.boe.es/eli/es/lo/2018/12/05/3

178 La loi espagnole va néanmoins plus loin que les dispositions prévues par RGPD en consacrant dans un chapitre X des disposions mentionnant la neutralité d'internet, l'accès universel d'internet, la sécurité numérique, l'éducation numérique, le droit à la vie privée et l'utilisation de dispositifs numériques sur le lieu de travail, le droit à la déconnexion numérique en dehors du lieu de travail, le droit à la vie privée contre l'utilisation de systèmes de géolocalisation sur le lieu de travail et également le droit à un testament numérique

179 Article 35.1 du Règlement Général sur la Protection des Données, https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016R0679

180 Les activités de traitement réalisées au moyen de technologies innovantes identifiées comme présentant un risque élevé pour les droits et libertés des personnes. Agencia Española de Protección de Datos, *Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD*, 21 juin 2019, consulté en ligne le 13.03.2020 à l'adresse suivante : https://www.aepd.es/sites/default/files/2019-09/guia-analisis-de-riesgos-rgpd.pdf

181 Agencia Española de Protección de Datos, *Orientaciones para centros educativos - Informe sobre la utilización por parte de profesores y alumnos de aplicaciones que almacenan datos en nube con sistemas ajenos a las plataformas educativas* , 6 mars 2018, §10 p. 9, consulté en ligne le 13.03.2020 à l'adresse suivante : https://www.aepd.es/sites/default/files/2019-09/guia-orientaciones-apps-datos-alumnos.pdf

182 *Ibidem.*

183 Agencia Española de Protección de Datos, *Guía sobre el uso de videocámaras para seguridad y otras finalidades*, « *La instalación de cámaras de videovigilancia en estos entornos con el fin de controlar conductas que puedan afectar a la seguridad, sólo será legítima cuando la medida sea proporcional en relación con la infracción que se pretenda evitar y, en ningún caso, debe suponer el medio inicial para llevar a cabo funciones de vigilancia.* », p. 39, 29 juin 2018, consulté en ligne le 13.03.2020 à l'adresse suivante : https://www.aepd.es/sites/default/files/2019-09/guia-videovigilancia.pdf

correspondre au « minimum nécessaire » couvrant les espaces publics tels que les accès ou les couloirs ; sont exclus de cette zone les espaces protégés par le droit à la vie privée comme les toilettes, les vestiaires ou les gymnases[184]. Enfin, la reconnaissance faciale ne peut être utilisée à des fins de contrôle de la fréquentation scolaire[185].

III. Cas d'usage

Dans l'espace public, trois terrains d'expérimentation ont été privilégiés en Espagne : les établissements scolaires (A), les contrôles aux frontières (B) et l'embarquement dans les aéroports (C).

A- La reconnaissance faciale et le contrôle de la fréquentation scolaire

Bien que les orientations de l'*Agencia Española de Protección de Datos* refusent l'usage de la reconnaissance faciale à des fins de contrôle de la fréquentation scolaire, plusieurs précédents espagnols ont été recensés en la matière. Ainsi, l'institut public de Badalona en Catalogne[186] fait usage d'un système de reconnaissance faciale pour contrôler la fréquentation des étudiants de première année ESO[187]. Le système est corrélé à l'envoi de SMS pour prévenir la famille de l'absence de leur enfant. Deux autres établissements scolaires espagnols ont utilisé la reconnaissance faciale pour réguler les passages à la cantine[188].

B - La reconnaissance faciale et le contrôle aux frontières

En juillet 2019, le Gouvernement de Sebta a mis en place un nouveau système de contrôle intelligent au poste de frontière de Sebta[189]. L'ambition est de créer une véritable "frontière intelligente" aux passages de Tarajal I et II pour assurer l'accélération du contrôle des transits tout en garantissant la sécurité, avec un contrôle plus efficace des durées de séjour. Cette initiative hispano-marocaine s'inscrit dans le programme « Gestion des flux et lutte contre la traite » et tend à renforcer le contrôle des frontières en les dotant notamment de dispositifs de reconnaissance faciale[190].

L'Union européenne a approuvé ce type de système de « frontières intelligentes » en 2017[191], mais ce n'est qu'en juillet 2019 que sa mise en œuvre fut lancée.

Le nouveau système d'entrée et de sortie (SES) implanté à Sebta prévoit la collecte de données des voyageurs de pays tiers lors du passage des personnes aux postes de frontières. La base de données est alimentée d'une photo du voyageur corrélée avec les informations contenues sur le document de voyage, les empreintes digitales, l'image faciale, la date et le lieu d'entrée et de sortie sur le territoire de l'espace Schengen. Les données sont ensuite conservées pendant trois ans et cinq ans pour les personnes ayant dépassé une durée maximale

184 *Ibidem* p. 40

185 *Ibidem.*

186 Badalona, Guia d'informació educativa de Badalona [en ligne], 2019, [consulté le 16/01/2020], http://badalona.cat/portalWeb/getfile?dID=105914&rendition=Web

187 La première année ESO correspond à la classe de sixième dans le système français

188 A. Asenjo, « Un instituto catalán está usando reconocimiento facial para controlar la asistencia a clase, algo por lo que ha sido multado con 19.000 euros un colegio sueco » [en ligne], *Business Insider*, 19 septembre 2019, [consulté le 16/01/2020], https://www.businessinsider.es/instituto-catalan-usa-reconocimiento-facial-asistencia-484683

189 Médias, « L'Espagne teste le système de reconnaissance faciale à Sebta » [en ligne], *Médias24* 24, 17 juillet 2019, [consulté le 16/01/2020], https://www.medias24.com/l-espagne-teste-le-systeme-de-reconnaissance-faciale-a-sebta-3561.html

190 N. Bernoussi, M. Benkeroum, « Maroc », Annuaire international de justice constitutionnelle, 32-2016, 2017, Migrations internationales et justice constitutionnelle - Référendums et justice constitutionnelle, p 428, site *Persée,* [consultation le 16/01/2020] https://www.persee.fr/doc/aijc_0995-3817_2017_num_32_2016_2529

191 Parlement Européen, « Schengen : des frontières intelligentes pour une meilleure protection (vidéo) », 25 octobre 2017, [consulté le 16/01/2020] https://www.europarl.europa.eu/news/fr/headlines/security/20171023STO86604/schengen-des-frontieres-intelligentes-pour-une-meilleure-protection-video

de séjour. La durée de conservation est justifiée par la possibilité de consulter ces informations dans le cadre d'enquêtes[192].

La frontière de Tarajal est considérée comme l'une des plus fréquentées au sein de l'Union européenne, avec un passage quotidien estimé à plus de 15 000 personnes. En 2018, selon les données marocaines, le renforcement effectué du contrôle à la frontière a permis d'arrêter 68000 tentatives de sortie et le démantèlement de 122 réseaux de traite des êtres humains[193].

Cependant, depuis octobre 2019, le projet, bien que venant d'une initiative européenne, rencontre des difficultés dans ses développements[194].

C - La reconnaissance faciale et l'embarquement à l'aéroport

En 2019, la compagnie aérienne espagnole Iberia a proposé une application mobile de reconnaissance faciale[195]. Il est dorénavant possible d'embarquer à bord de l'un de ses vols en partance du terminal 4 de l'aéroport Adolfo Suárez de Madrid-Barajas et à destination de Bruxelles ou des Asturies grâce au système de reconnaissance faciale prévu par son application mobile. L'utilisation de cette technologie commence par la création d'un compte. Pour cela, le voyageur est invité à télécharger sa pièce d'identité sur l'application Iberia. Puis, ce dernier doit se prendre en selfie afin que le logiciel vérifie la correspondance entre la vidéo et la photo préalablement enregistrées. Le profil biométrique complet, celui-ci est soumis à la base de données de l'exploitant d'aéroport. Pour s'enregistrer en ligne, le passager doit ensuite associer sa carte d'embarquement à son profil biométrique ; la reconnaissance faciale lui permet alors d'effectuer le contrôle de sécurité et passer les portes d'embarquement.

Le système d'Iberia est encore assez restrictif : départ et arrivée sont limités, et seuls les passagers détenteurs d'un document national espagnol version 3.0 ou d'un passeport européen peuvent en bénéficier. De plus, l'application est, pour l'heure, uniquement disponible sur le système d'exploitation d'Android.

192 M. Jimenez, « Reconocimiento facial en la nueva 'frontera inteligente' con Marruecos », *El Imparcial*, 17 juillet 2019, [consulté le 16/01/2020] https://www.elimparcial.es/noticia/203269/sociedad/el-reconocimiento-facial-llega-a-la-nueva-frontera-inteligente-con-marruecos.html

193 Gouvernement Espagnol, « Repuesta del Gobierno », 2 septembre 2019, http://www.congreso.es/l13p/e0/e_0005331_n_000.pdf

194 A. Abjiou, « Sebta: Le projet espagnol de frontière intelligente prend l'eau » [en ligne], *L'Economiste*, 18 octobre 2019, [consulté le 16/01/2020], https://www.leconomiste.com/article/1051924-sebta-le-projet-espagnol-de-frontiere-intelligente-prend-l-eau

195 Business Traveler, « Iberia teste une application de reconnaissance faciale » [en ligne], *Business Traveler*, 26 novembre 2019, [consultation le 16/01/2020], https://www.businesstravel.fr/iberia-teste-une-application-de-reconnaissance-faciale.html

BIBLIOGRAPHIE

I. Législation

- Loi organique n°3/2018 du 5 décembre 2018, https://www.boe.es/eli/es/lo/2018/12/05/3
- Article 35.1 du Règlement Général sur la Protection des Données, https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016R0679

II. Prise de position des autorités régulatrices de la protection des données

- Agencia Española de Protección de Datos, *Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD*, 21 juin 2019, consulté en ligne le 13.03.2020 à l'adresse suivante : https://www.aepd.es/sites/default/files/2019-09/guia-analisis-de-riesgos-rgpd.pdf

- Agencia Española de Protección de Datos, *Guía sobre el uso de videocámaras para seguridad y otras finalidades*, 29 juin 2018, consulté en ligne le 13.03.2020 à l'adresse suivante : https://www.aepd.es/sites/default/files/2019-09/guia-videovigilancia.pdf

- Agencia Española de Protección de Datos, *Orientaciones para centros educativos - Informe sobre la utilización por parte de profesores y alumnos de aplicaciones que almacenan datos en nube con sistemas ajenos a las plataformas educativas*, 6 mars 2018, consulté en ligne le 13.03.2020 à l'adresse suivante : https://www.aepd.es/sites/default/files/2019-09/guia-orientaciones-apps-datos-alumnos.pdf

III. Presse numérique

- ABJIOU A., « Sebta: Le projet espagnol de frontière intelligente prend l'eau », *L'Economiste*, 18 octobre 2019, consulté en ligne le 16.01.2020 à l'adresse suivante : https://www.leconomiste.com/article/1051924-sebta-le-projet-espagnol-de-frontiere-intelligente-prend-l-eau
- ASENJO A., « Un instituto catalán está usando reconocimiento facial para controlar la asistencia a clase, algo por lo que ha sido multado con 19.000 euros un colegio sueco » [en ligne], *Business Insider*, 19 septembre 2019, consulté en ligne le 16.01.2020 à l'adresse suivante : https://www.businessinsider.es/instituto-catalan-usa-reconocimiento-facial-asistencia-484683
- Badalona, *Guia d'informació educativa de Badalona*, 2019, consulté en ligne le 16.01.2020 à l'adresse suivante : http://badalona.cat/portalWeb/getfile?dID=105914&rendition=Web

- BERNOUSSI N. et BENKEROUM M., « Maroc », Annuaire international de justice constitutionnelle, 32-2016, 2017, Migrations internationales et justice constitutionnelle - Référendums et justice constitutionnelle, p 428, *Persée,* consulté en ligne le 16.01.2020 à l'adresse suivante : https://www.persee.fr/doc/aijc_0995-3817_2017_num_32_2016_2529

- Business Traveler, « Iberia teste une application de reconnaissance faciale », *Business Traveler*, 26 novembre 2019, consulté en ligne le 16.01.2020 à l'adresse suivante : https://www.businesstravel.fr/iberia-teste-une-application-de-reconnaissance-faciale.html

- Gouvernement Espagnol, « Repuesta del Gobierno », 2 septembre 2019, consulté en ligne le 16.01.2020 à l'adresse suivante : http://www.congreso.es/l13p/e0/e_0005331_n_000.pdf

- JIMENEZ M., « Reconocimiento facial en la nueva 'frontera inteligente' con Marruecos », *El Imparcial*, 17 juil-

let 2019, consulté en ligne le 16.01.2020 à l'adresse suivante : https://www.elimparcial.es/noticia/203269/sociedad/el-reconocimiento-facial-llega-a-la-nueva-frontera-inteligente-con-marruecos.html

- Médias, « L'Espagne teste le système de reconnaissance faciale à Sebta », *Médias 24*, 17 juillet 2019, consulté en ligne le 16.01.2020 à l'adresse suivante : https://www.medias24.com/l-espagne-teste-le-systeme-de-reconnaissance-faciale-a-sebta-3561.html

- Parlement Européen, « Schengen : des frontières intelligentes pour une meilleure protection (video) » 25 octobre 2017, consulté en ligne le 16.01.2020 à l'adresse suivante : https://www.europarl.europa.eu/news/fr/headlines/security/20171023STO86604/schengen-des-frontieres-intelligentes-pour-une-meilleure-protection-video

France

I. Législation

La France ne dispose pas de régime juridique propre à l'utilisation des technologies de reconnaissance faciale. De tels dispositifs doivent néanmoins se conformer à la législation relative à la protection des données d'une part (**A**) ; aux dispositions du Code de la Sécurité Intérieure relatives à la vidéo protection de l'autre (**B**).

A - Législation française relative à la protection des données

Le débat public plébiscite l'adoption d'une loi spéciale encadrant des déploiements **ciblés**[196]. Toutefois ce cadre spécifique fait défaut à ce jour. Les dispositifs de reconnaissance faciale relèvent aussi du droit commun prévu par la loi du 6 janvier 1978[197] relative à l'informatique, aux fichiers et aux libertés (LIL), récemment enrichie par la loi du 20 juin 2018[198] et l'ordonnance du 12 décembre 2018[199].

L'interconnexion des bases de données biométriques avec des dispositifs de reconnaissance faciale tombe sous le joug de l'article 6 de LIL[200]. Les articles 31(II)[201] et 32[202] conditionnent les traitements de données « sensibles » pour le compte de l'État, à l'adoption d'un décret en Conseil d'État. Le déploiement de dispositifs de reconnaissance faciale dans l'espace public, à des fins de prévention des troubles à l'ordre public, doit donc être autorisé par décret en Conseil d'État, après avis motivé et publié de la Commission Nationale de l'Informatique et des Libertés (CNIL).

B - Dispositions spécifiques applicables à la mise en place des caméras de vidéoprotection

La reconnaissance faciale nécessite, pour être mise en œuvre, l'indexation de bases de données aux caméras de vidéoprotection. Par ailleurs, les logiciels peuvent être intégrés directement sur les caméras déjà existantes. Dès lors, l'installation et le recours à de tel dispositifs de surveillance doivent se conformer aux obligations posées par le **Code de la Sécurité Intérieure** (ci-après « **CSI ») ** en matière d'installation de caméras à des fins de vidéoprotection[203].

L'article L252-1 alinéa 2 du CSI subordonne la mise en place des systèmes de vidéoprotection à une autorisation préfectorale après avis de la Commission départementale de la vidéoprotection. La CNIL doit autoriser ce traitement lorsque les systèmes de vidéosurveillance sont « utilisés sur la voie publique ou dans des lieux ouverts au public dont les enregistrements sont utilisés dans des traitements automatisés ou contenus

196 A titre d'exemple, la proposition de loi relative à la reconnaissance faciale dans les enquêtes terroristes et la prévention des attentats, déposée par la Députée Marine Brenier en septembre 2017

197 Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés Version consolidée au 18 mars 2020,
https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460

198 Portant adaptation de la législation nationale pour donner suite à l'entrée en vigueur du RGPD Loi n°2018-493, 20 juin 2018 relative à la protection des données.
https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000037085952&categorieLien=id

199 Prise en application de l'article 32 de la loi précitée. Ordonnance n°2018-1125, 12 décembre 2018,
https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000037800506&categorieLien=id

200 Cet article, en ses deux premiers alinéas, transpose de l'article 9 du RGPD.

201 Article 31(II) : « II.-*Ceux de ces traitements qui portent sur des données mentionnées au I de l'article 6 sont autorisés par décret en Conseil d'Etat pris après avis motivé et publié de la commission. Cet avis est publié avec le décret autorisant le traitement* ».

202 Article 32 : « *Sont autorisés par décret en Conseil d'Etat, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés, les traitements de données à caractère personnel mis en œuvre pour le compte de l'Etat, agissant dans l'exercice de ses prérogatives de puissance publique, qui portent sur des données génétiques ou sur des données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes.* »

203 Ce sont les articles **L251-1 à L255-1 ainsi que les articles L223-1 à L223-9 en matière de lutte contre le terrorisme et les atteintes aux intérêts fondamentaux de la nation** du Code de la Sécurité intérieure qui visent à s'appliquer en complément des dispositions propres à la protection des données personnelles.

dans des fichiers structurés selon des critères permettant d'identifier, directement ou indirectement, des personnes physiques »[204].

En dehors des cas précités, le Préfet et la commission départementale de la vidéoprotection restent compétents au titre de **l'article L252-1 alinéa 1 du CSI**.

II. Position de l'autorité de contrôle

Le 15 novembre 2019, la CNIL a publié un rapport sur la reconnaissance faciale[205]. La commission rappelle le cadre juridique qui entoure l'utilisation de cette technologie. Elle ne formule pas un avis général tranché, mais des exigences pour la mise en œuvre des dispositifs. Il appartient à toute autorité désireuse de mettre en œuvre une expérimentation de :

- Tracer des lignes rouges préalablement à tout usage expérimental de la reconnaissance faciale. Ce bornage résultera nécessairement d'une approche concertée entre pouvoirs publics et la CNIL à travers son rôle de conseil.
- Respecter les droits et libertés des personnes ; aussi, en dehors de l'encadrement juridique, « les expérimentations ne sauraient éthiquement avoir pour objet ou pour effet d'accoutumer les personnes à des techniques de surveillance intrusive » ;
- Adopter une démarche « véritablement expérimentale ». Il s'agit d'éviter « tout effet cliquet lié à la mise en œuvre de certains dispositifs ». La Quadrature du net, interrogé dans le cadre de ce rapport redoute en ce sens que l'expérimentation conduise à la banalisation *ex post* de la technologie[206].

La CNIL invite le législateur à se prononcer sur la reconnaissance faciale et forme de ses vœux la tenue d'un « débat à la hauteur des enjeux ».

Les cas d'usages de la reconnaissance faciale se multiplient en France. La Commission a eu l'occasion d'émettre son avis sur certains d'entre eux[207]. Nous étudierons ceux-ci dans l'étude de cas ci-dessous.

III. Cas d'usage

En France, les terrains d'expérimentations sont multiples. Le recours à la reconnaissance faciale a concerné aussi bien les événements festifs, notamment lors du Carnaval de Nice en 2019 (**A**), les établissements scolaires (**B** donnant lieu à un recours contentieux. Plusieurs expérimentations ont également vu le jour dans le cadre du système PARAFE (**C**), dans la continuité de ce qui se développe de manière croissante au sein de l'Union. Enfin, la sécurisation des enceintes sportive demeure une thématique intrinsèquement liée au développement de la technologie comme en témoignent les tests réalisés au stade de Metz (**D**).

A - Expérimentation lors du carnaval de Nice

Ce cas constitue la première expérimentation[208] de reconnaissance faciale sur la voie publique en France. Elle s'est tenue les 16, 19 et 20 février 2019 à l'occasion de la 135e édition du carnaval de Nice. C'est la société monégasque Confidentia qui mit à disposition de la ville la solution de reconnaissance faciale de l'entreprise israélienne Anyvision. La particularité de ce logiciel est la possibilité de l'intégrer sur des systèmes de vidéoprotection préexistants.

---

204 Article L252-1 alinéa 2 du Code de la Sécurité Intérieure

205 « Reconnaissance faciale : pour un débat à la hauteur des enjeux », *Rapport de la Commission Nationale de l'Informatique et des Libertés*, novembre 2019, 11p, [consulté le 01/02/2020], https://www.cnil.fr/sites/default/files/atoms/files/reconnaissance_faciale.pdf

206 Voy. nos entretiens en annexe.

207 Ces prises de positions s'expliquent en partie du fait de l'ampleur et de la forte médiatisation de certains cas d'usages.

208 « Expérimentation reconnaissance faciale », *rapport de la ville de Nice*, 2019, https://www.documentcloud.org/documents/6350838-Bilan-Reconnaissance-Faciale.html

Plusieurs agents de la collectivité ont été volontaires pour servir de testeur[209]. Près de 5000 personnes ont passé les portiques accueillant le dispositif de reconnaissance faciale.

Deux scénarios ont été testés :

- ⇨ D'une part, un contrôle d'accès « un par un ». Dans ce cas de figure, le logiciel présentait la capacité de reconnaître les personnes autorisées ou non à intégrer la zone ainsi que la file d'attente.
- ⇨ D'autre part, le contrôle « à la volée », permettant de détecter une personne présente dans la foule. Dans cette situation, le Centre de Supervision Urbain était directement en relation avec les agents sur le terrain, pour les informer lors de la reconnaissance d'une personne d'intérêt.

Sur ce cas, la CNIL s'est exprimée publiquement en réaction aux propos tenus par la Ville de Nice sur le réseau social Twitter. Cette dernière considérait que la CNIL avait autorisé le traitement.

La CNIL a d'abord rappelé que, depuis l'entrée en vigueur du RGPD l'autorisation préalable n'est plus une condition préalable requise à la mise en place d'une expérimentation. Elle regrettait toutefois l'urgence dans laquelle ses services avaient été sollicités : cette situation ne permettait pas une analyse approfondie du projet.

Ensuite, la finalité de recherche scientifique de l'expérimentation faisait reposer sur le projet sur consentement des personnes volontaires pour y participer. Elle indiquait aussi être vigilante quant aux garanties mises en place pour en assurer la validité.

La CNIL rappelait enfin que le cadre juridique actuel, dépourvu de dispositions spécifique à la reconnaissance faciale, ne pouvait permettre la poursuite de l'expérimentation ; il appartenait à la commune de lui remettre un rapport détaillé de l'expérimentation. En juillet 2019, celui-ci a été communiqué par la ville de Nice. Le régulateur a fait une demande d'information complémentaire par un courrier du 16 juillet 2019. Ce rapport a été publié par le journal Le Monde le 28 août 2019[210].

B - Projet d'expérimentation de la reconnaissance faciale dans les lycées

Le 8 avril 2016, l'Assemblée Plénière du Conseil Régional de la région Provence Alpes Côte Azur (PACA) a voté un plan de mise en sûreté des lycées prévoyants « d'assurer des conditions de travail à la communauté éducative et aux lycéens qui soient les plus sécurisés possibles ». C'est dans ce contexte que, depuis 2016, 1300 caméras de vidéoprotection ont été installées dans les lycées de la région PACA.

Le 20 octobre 2017, le Président de la région transmettait à la Commission Nationale de l'Informatique et des Libertés un courrier détaillant le projet[211], complété, à la demande de la CNIL, par un second courrier en date du 7 mars 2018[212]. Le dispositif concernait de deux lycées de la région à Nice (Les Eucalyptus) et Marseille (Ampère).

Dans sa délibération en date du 14 décembre 2018,[213] le **Conseil Régional de la région PACA** a autorisé la mise en place du dispositif de « contrôle d'accès virtuel dans les lycées ». D'après les informations contenues dans l'exposé du projet, l'expérimentation visait à « évaluer la valeur ajoutée, mais aussi les contraintes

209 « Expérimentation reconnaissance faciale », rapport de la ville de Nice, 2019, https://www.documentcloud.org/documents/6350838-Bilan-Reconnaissance-Faciale.html

210 M.Untersinger, « Reconnaissance faciale : la CNIL tique sur le bilan de l'expérience niçoise », [en ligne], *Le Monde*, 28 août 2019, [consulté en ligne le 01/02/2020], https://www.lemonde.fr/pixels/article/2019/08/28/reconnaissance-faciale-la-cnil-tique-sur-le-bilan-de-l-experience-nicoise_5503769_4408996.html

211 Lettre de Renaud Muselier, https://www.laquadrature.net/wp-content/uploads/sites/8/2018/12/1545041938824-1_dc-17021806-20-oct-2017.pdf

212 La Quadrature du net, « Demande de compléments projet « portiques virtuels » Provence-Alpes-Côte d'Azur » [en ligne], *La Quadrature du net*, le 7 mars 2018, [consulté le 01/02/2020], https://www.laquadrature.net/wp-content/uploads/sites/8/2018/12/1545041927219-dem-compl-projet-portique-virtuel-lyc%C3%A9es.pdf

213 Délibération n°18-893 du 14 décembre 2018, https://www.laquadrature.net/wp-content/uploads/sites/8/2019/02/4.-D%C3%A9lib%C3%A9ration-attaqu%C3%A9e.pdf

opérationnelles qu'impliquerait la mise en œuvre d'un dispositif de comparaison faciale au sein d'un lycée »[214]. La finalité du traitement était la fluidification des flux à l'entrée des lycées, la lutte contre les cas d'usurpation d'identité et la détection et l'alerte de déplacements non autorisés dans l'établissement. Une version finalisée de l'Analyse d'Impact relative à la Protection des Données a été transmise à la CNIL durant le mois de juillet 2019.

Ce « projet de portique de sécurité virtuel » reposait sur la mise en place de « **portiques visuels** » associant des méthodes d'identification traditionnelles à des dispositifs biométriques basés sur un algorithme de reconnaissance faciale. Au-delà de la comparaison faciale, le dispositif réalisait un suivi de trajectoire. La maîtrise d'œuvre de l'expérimentation devait être assurée par la société Cisco.

Afin de garantir l'efficacité du dispositif expérimental, deux **bases de données** devaient être constituées.

- Dans la première devaient être compilées les noms, prénoms et identifiants numériques des personnes concernées sous la forme d'un badge QR code ou grâce à l'utilisation de la technologie *Near Field Communication* (NFC).

- La seconde devait contenir le gabarit biométrique des personnes concernées, gabarit créé lors de leur enrôlement de ces dernières et rattaché à leur identifiant numérique.

Le logiciel comparerait ensuite le visage obtenu en temps réel par la caméra du portique avec le gabarit contenu dans le support physique présenté au lecteur de badge. Dans l'hypothèse où la personne filmée par la caméra ne correspondait pas avec l'identifiant numérique, un message d'alerte devait être envoyé aux agents de l'établissement.

L'expérimentation envisagée dans les lycées devait également concerner un dispositif de détection des intrusions. Dans ce cas, le logiciel d'intelligence artificielle fonctionnant sur la base de l'ensemble des caméras de l'établissement aurait procédé à un suivi de trajectoire des personnes entrantes. Le logiciel devait permettre, grâce aux images de vidéosurveillance de l'établissement, de détecter le visage des individus et de leur attribuer une couleur spécifique.

Trois possibilités étaient alors envisagées[215] :

- La couleur verte, dans le cas où le visage de la personne filmée correspondait au gabarit contenu dans le badge ;
- La couleur jaune « visiteur », si la personne ne disposait pas de badge. Dans une telle hypothèse, la personne devait se signaler et s'enregistrer au risque de passer en catégorie rouge ;
- La couleur rouge visait les personnes n'ayant pas de badge ou celles ayant tenté de dissimuler leur visage.

L'expérimentation, qui ne s'est finalement pas tenue, devait avoir lieu pendant une durée de **six mois.** Le recueil des données reposait sur le **consentement** des personnes concernées si ces derniers étaient majeurs, ou de leur représentant légal pour les mineurs. Un formulaire de recueil de consentement devait être signé par toutes les personnes intéressées par le traitement expérimental des données.

Pour les personnes extérieures à l'expérimentation, des panneaux d'affichage étaient installés « à la périphérie des zones concernées » les informant de la finalité de l'expérimentation et du moyen d'exercer leurs droits. Une notice d'information devait en outre indiquer un chemin alternatif permettant de ne pas faire l'objet du traitement expérimental.

Enfin, seules les personnes habilitées et tenues à un engagement de confidentialité pouvaient accéder aux données, qui ne seraient conservées que pendant la durée de l'expérimentation.

---

214 La Quadrature du net, « Expérimentation « portique virtuel » dans deux lycées de la région Provence-Alpes-Côte d'Azur » [en ligne], *La Quadrature du net*, 20 décembre 2018, [consulté le 01/02/2020], https://www.laquadrature.net/wp-content/uploads/sites/8/2018/12/1545041934529-2_exp%C3%A9_portique_virtuel_lyc%C3%A9es.pdf

215 R. Baheux, « La reconnaissance faciale testée dans des lycées » [en ligne], *Le Parisien*, 4 février 2019, [consultée le 01/02/2020], http://www.leparisien.fr/societe/video-dans-les-lycees-et-maintenant-place-a-la-reconnaissance-faciale-04-02-2019-8004192.php

Délibération de la CNIL. Lors d'une séance plénière du 17 octobre 2019[216], la Commission Nationale de l'Informatique et des Libertés a également eu l'occasion de se prononcer sur le projet de mise en place d'un dispositif de reconnaissance faciale à l'entrée de deux lycées de la région sud. Dans un communiqué du 29 octobre 2019, l'autorité de contrôle française a « considéré que le dispositif projeté est contraire aux grands principes de proportionnalité et de minimisation des données posés par le RGPD », soulignant le caractère particulièrement intrusif des dispositifs de reconnaissance et la sensibilité des données nécessaires à son fonctionnement.

Les objectifs poursuivis lors de l'expérimentation pouvaient, selon la CNIL, être atteints par des moyens « bien moins intrusifs ». La Commission considéra également une augmentation notable des risques pesant sur la vie privée et les libertés individuelles. En raison d'un traitement de données à destination de personnes mineures, celui-ci devait bénéficier « d'une protection particulière dans les textes nationaux et européens ».

Recours. La délibération de la Région Sud autorisant le dispositif fit l'objet d'un recours devant le Tribunal administratif de Marseille par la Quadrature du Net et d'autres acteurs locaux[217]. Le **Tribunal Administratif de Marseille[218] s'est prononcé 27 février 2020**. Cette décision constitue la **première décision juridictionnelle française** relative à la reconnaissance faciale.

Le Tribunal considéra que la région était incompétente pour encadrer et surveiller les élèves : « les missions d'encadrement et de surveillance des élèves qui ressortissent à la compétence des chefs d'établissements (...) ». En sus de l'illégalité externe de la délibération, les juges soulevèrent également l'illégalité de l'acte sur le fondement de l'article 9 du RGPD. Le consentement ne pouvait être considéré comme libre et éclairé au regard de la situation d'autorité entre les élèves et l'établissement public d'enseignement.

C - Le système PARAFE (Passage Automatisé Rapide Aux Frontières extérieures)

Le système PARAFE est un système d'authentification par reconnaissance facial mis en place dans le cadre du contrôle aux frontières.

Cent deux sas PARAFE ont été mis en place à Roissy Charles de Gaulle en 2009, ainsi qu'à l'aéroport d'Orly avant d'être modernisés en 2017 et 2018[219]. Initialement dépourvus de reconnaissance faciale, les sas PARAFE s'appuient aujourd'hui sur celle-ci[220]. L'image faciale vient compléter les mécanismes plus classiques de reconnaissance des empreintes biométriques. Pour rappel, depuis 2008, les passeports délivrés par l'Administration française sont équipés d'une puce électronique dans laquelle sont enregistrées la photographie et les empreintes digitales de deux doigts du titulaire du passeport ; cela permet d'établir les correspondances.

Par ailleurs, le dispositif PARAFE a également été déployé dans les aéroports de Marseille-Provence, Nice et Lyon Saint-Exupéry. Les gares ne sont pas en reste, puisque la Gare du Nord à Paris est également équipée du système PARAFE

Délibération de la CNIL. Dans sa délibération du 28 janvier 2016[221], elle relève deux points importants :

- Premièrement, que ce dispositif ne nécessitait pas la constitution d'une base de données centralisée ;

216 Commission Nationale de l'Informatique et des Libertés, « Expérimentation de la reconnaissance faciale dans deux lycées : la CNIL précise sa position » [en ligne], *CNIL*, 29 octobre 2019, [consulté le 01/02/2020], https://www.cnil.fr/fr/experimentation-de-la-reconnaissance-faciale-dans-deux-lycees-la-cnil-precise-sa-position

217 Recours devant le Tribunal Administratif de Marseille contre la délibération n° 18-893 du 14 décembre 2018 du Conseil régional Provence-Alpes-Côte d'Azur,concernant l'«Expérimentation du dispositif de contrôle d'accès virtuel dans les lycées »

218 TA Marseille, 27 février 2020, n°1901249 : https://www.laquadrature.net/wp-content/uploads/sites/8/2020/02/1090394890_1901249.pdf

219 Gemalto, « PARAFE : une nouvelle génération pour Roissy et Orly », [en ligne], 12 novembre 2019, [consulté le 01/02/2020], https://www.gemalto.com/france/gouv/biometrie-parafe

220 Ministère de L'Intérieur, « Passez les contrôles aux frontières plus rapidement avec PARAFE ! » [en ligne], Intérieur.gouv.fr, 16 juillet 2019, [consulté le 01/02/2020], https://www.interieur.gouv.fr/Actualites/Infos-pratiques/Passez-les-controles-aux-frontieres-plus-rapidement-avec-PARAFE

221 CNIL, Délibération n° 2016-012 du 28 janvier 2016 portant avis sur un projet de décret portant modification d'un traitement automatisé de données à caractère personnel dénommé PARAFE, https://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000032385417

les images recueillies dans le sas sont effacées dès la comparaison effectuée avec l'image numérisée stockée dans le passeport. En ce sens, il garantit une meilleure protection des données personnelles des personnes concernées.

- Deuxièmement, cette fonctionnalité repose sur le volontariat des passagers. Le dispositif est donc, selon elle, conforme à ses exigences. La commission estime toutefois que le projet de décret offre une « base pérenne » pour le déploiement généralisé de PARAFE, ne lui permettant pas d'analyser a posteriori cette expérimentation. Cette nouvelle modalité d'authentification des personnes a d'ailleurs été confirmée et officialisée dans un décret publié au Journal Officiel le 8 avril 2016[222].

D - Dispositif de reconnaissance faciale au sein du stade de Football du FC Metz

Le stade Saint-Symphorien du FC Metz a testé un dispositif de reconnaissance faciale proposé par la *start up* messine Two-i[223]. En l'état actuel des informations, la solution n'a pas été déployée à grande échelle sur les supporters, et ne consiste qu'en des tests sur les salariés de l'entreprise.

En tout état de cause, le logiciel testé devrait permettre de faire respecter les dispositions de la loi du 10 mai 2016[224] dite Larrivé, concernant la sécurité des manifestations sportives, notamment les interdictions d'entrée au sein des enceintes sportives. Cette loi prévoit des mesures particulières d'interdictions à l'encontre des personnes faisant l'objet d'une interdiction judiciaire (article L332-11)[225] ou administrative (L332-16)[226] concernant la fréquentation de ce stade.

---

222 Décret n°2016-414 du 6 avril 2016 portant modification d'un traitement automatisé de données à caractère personnel dénommé « PARAFE », https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000032372112&categorieLien=id

223 J-L Mounier, « La reconnaissance faciale au FC Metz, une expérimentation qui suscite la controverse » [en ligne], 2 février 2020, [consulté le 18/03/2020], https://www.france24.com/fr/20200202-la-reconnaissance-faciale-au-fc-metz-une-exp%C3%A9rimentation-qui-suscite-la-controverse

224 LOI n° 2016-564 du 10 mai 2016 renforçant le dialogue avec les supporters et la lutte contre le hooliganisme

225 « *Les personnes coupables de l'une des infractions définies aux articles L. 332-3 à L. 332-10 et L. 332-19 du présent code encourent également la peine complémentaire d'interdiction de pénétrer ou de se rendre aux abords d'une enceinte où se déroule une manifestation sportive, pour une durée qui ne peut excéder cinq ans. La personne condamnée à cette peine est astreinte par le tribunal à répondre, au moment des manifestations sportives, aux convocations de toute autorité ou de toute personne qualifiée que la juridiction désigne dans sa décision. Cette décision peut prévoir que l'obligation de répondre à ces convocations s'applique au moment de certaines manifestations sportives, qu'elle désigne, se déroulant sur le territoire d'un Etat étranger.*
Cette peine complémentaire est également applicable aux personnes coupables de l'une des infractions définies aux articles 222-11 à 222-13, 322-1 à 322-4, 322-6, 322-11 et 433-6 du code pénal lorsque cette infraction a été commise dans une enceinte où se déroule une manifestation sportive ou, à l'extérieur de l'enceinte, en relation directe avec une manifestation sportive. »

226 « *Lorsque, par son comportement d'ensemble à l'occasion de manifestations sportives, par la commission d'un acte grave à l'occasion de l'une de ces manifestations, du fait de son appartenance à une association ou un groupement de fait ayant fait l'objet d'une dissolution en application de l'article L. 332-18 ou du fait de sa participation aux activités qu'une association ayant fait l'objet d'une suspension d'activité s'est vue interdire en application du même article, une personne constitue une menace pour l'ordre public, le représentant de l'Etat dans le département et, à Paris, le préfet de police peuvent, par arrêté motivé, prononcer à son encontre une mesure d'interdiction de pénétrer ou de se rendre aux abords des enceintes où de telles manifestations se déroulent ou sont retransmises en public.[…]* »

BIBLIOGRAPHIE

I. Législation

- Décret n°2016-414 du 6 avril 2016 portant modification d'un traitement automatisé de données à caractère personnel dénommé « PARAFE », https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000032372112&categorieLien=id

- Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés Version consolidée au 18 mars 2020, https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460

- Loi n°2018-493, 20 juin 2018 relative à la protection des données, https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000037085952&categorieLien=id

- Ordonnance n°2018-1125, 12 décembre 2018, https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000037800506&categorieLien=id

II. Prise de position de l'autorité de contrôle de la protection des données

- CNIL, Délibération n° 2016-012 du 28 janvier 2016 portant avis sur un projet de décret portant modification d'un traitement automatisé de données à caractère personnel dénommé PARAFE, https://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000032385417

- CNIL, « Expérimentation de la reconnaissance faciale dans deux lycées : la CNIL précise sa position » [en ligne], *CNIL*, 29 octobre 2019, [consulté le 01/02/2020], https://www.cnil.fr/fr/experimentation-de-la-reconnaissance-faciale-dans-deux-lycees-la-cnil-precise-sa-position

- « Reconnaissance faciale : pour un débat à la hauteur des enjeux », *Rapport de la Commission Nationale de l'Informatique et des Libertés*, novembre 2019, 11p, [consulté le 01/02/2020], https://www.cnil.fr/sites/default/files/atoms/files/reconnaissance_faciale.pdf

III. Presse numérique

- AFP, « Test de reconnaissance faciale à Nice: précisions de la CNIL », *Public Sénat*, le 19 février 2019, [consulté le 30/01/2020], https://www.publicsenat.fr/article/politique/test-de-reconnaissance-faciale-a-nice-precisions-de-la-cnil-138122

- Baheux R, « La reconnaissance faciale testée dans des lycées » [en ligne], Le Parisien, 4 février 2019, [consultée le 01/02/2020], http://www.leparisien.fr/societe/video-dans-les-lycees-et-maintenant-place-a-la-reconnaissance-faciale-04-02-2019-8004192.php

- Gemalto, « PARAFE : une nouvelle génération pour Roissy et Orly », [en ligne], 12 novembre 2019, [consulté 01/02/2020], https://www.gemalto.com/france/gouv/biometrie-parafe

- Mounier J-L, « La reconnaissance faciale au FC Metz, une expérimentation qui suscite la controverse » [en ligne], 2 février 2020, [consulté le 18/03/2020], https://www.france24.com/fr/20200202-la-reconnaissance-faciale-au-fc-metz-une-exp%C3%A9rimentation-qui-suscite-la-controverse

- La Quadrature du net, « Expérimentation « portique virtuel » dans deux lycées de la région Provence-Alpes-Côte d'Azur » [en ligne], *La Quadrature du net*, 20 décembre 2018, [consulté le 01/02/2020], https://www.laquadrature.net/wp-content/uploads/sites/8/2018/12/1545041934529-2_exp%C3%A9_portique_virtuel_lyc%C3%A9es.pdf
- La Quadrature du net, « Demande de compléments projet « portiques virtuels » Provence-Alpes-Côte d'Azur » [en ligne], *La Quadrature du net*, le 7 mars 2018, [consulté le 01/02/2020],https://www.laquadrature.net/wpcontent/uploads/sites/8/2018/12/1545041927219-dem-compl-projet-portique-virtuel-lyc%C3%A9es.pdf
- Paris Aéroport, « Contrôle aux frontières avec PARAFE » [en ligne], *Paris Aéroport*, [consulté le 01/02/2020], https://www.parisaeroport.fr/passagers/preparation-vol/votre-voyage/controle

- Untersinger M, « Reconnaissance faciale : la CNIL tique sur le bilan de l'expérience niçoise », [en ligne], Le Monde, 28 août 2019, [consulté en ligne le 01/02/2020], https://www.lemonde.fr/pixels/article/2019/08/28/reconnaissance-faciale-la-cnil-tique-sur-le-bilan-de-l-experience-nicoise_5503769_4408996.html

Italie

I. Législation

En Italie, il n'y a pas de législation spécifique encadrant l'utilisation de la reconnaissance faciale. Cependant, deux textes nationaux et généraux sur le traitement des données personnelles transposent respectivement la Directive Police Justice et le RGPD, et posent ainsi les premiers jalons d'un encadrement légal de la technologie : **le décret législatif du 18 mai 2018, n°51 et le décret législatif du 10 août 2018, n°101**.

Ils sont complétés par différentes dispositions réglementent le traitement des données biométriques **par la police** - à des fins de prévention, d'enquête, de détection et de poursuite des délits ou d'exécution de sanctions pénales – à l'instar de l'article 4 du *Testo unico delle leggi di pubblica sicurezza*[227], l'article 11 de la loi du 18 mai 1978 et l'article 5 du décret législatif du 25 juillet 1998 n°286 [228].

Le traitement de données biométriques par les forces de police est également décrit par le décret du ministre de l'Intérieur du 24 mai 2017, en application de l'article 53 § 3 du code italien de protection des données personnelles. Sa base juridique est établie par l'article 49 du décret législatif du 18 mai 2018, n°51 : ce dernier prévoit que l'article 53 du code est abrogé, mais que les décrets adoptés conformément à cet article continuent de s'appliquer dans l'attente de l'adoption de nouvelles règles[229].

II. La position de l'autorité de contrôle

Dans sa décision n°9040256 du 26 juillet 2018[230], l'Agence italienne pour la protection des données s'est prononcée sur l'utilisation par la police d'un logiciel de reconnaissance faciale en différé. L'autorité de contrôle s'est concentrée sur deux points de droit : la nécessité du traitement et l'interdiction des décisions fondées uniquement sur un traitement automatisé.

Premièrement, l'autorité juge le traitement de données biométriques conforme aux exigences de l'article 7 du décret législatif du 18 mai 2018, qui exige la stricte nécessité du traitement ainsi que des garanties adéquates pour les droits et libertés. En particulier, l'Agence italienne pour la protection des données a estimé que « la stricte nécessité du traitement est confirmée en raison de la fonctionnalité de ce système par rapport aux activités d'identification menées par les forces de police »[231].

Deuxièmement, ce traitement de données sensibles ne tombe pas sous le coup de l'interdiction des décisions fondées uniquement sur un traitement automatisé prévue à l'article 8 du décret législatif du 18 mai 2018. Le régulateur italien a estimé que ce logiciel est une « simple aide à l'action humaine, visant à accélérer l'identification par le policier d'une personne recherchée dont l'image faciale est disponible, sans préjudice de la nécessité pour le policier de vérifier la fiabilité des résultats produits par le système automatisé »[232].

Par ailleurs dans une décision n°8789277[233], rendue dans le cadre d'une consultation préalable, l'autorité italienne s'est positionnée sur l'utilisation de la reconnaissance faciale dans les aéroports à des fins

---

227 Article 349 du Code italien de procédure pénale.

228 Garante Per la Protezione Dei Dati **« Personali, Sistema automatico di ricerca dell'identità di un volto », 26 juillet 2018, n°9040256**, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9040256

229 Decreto Legislativo, 18 mai 2018, n°51, Articolo 49, https://www.gazzettaufficiale.it/eli/id/2018/05/24/18G00080/sg

230 Garante Per La Protezione Dei Dati Personali, Décision n°9040256 rendue le 26 juillet 2018.

231 *« L'ulteriore requisito - previsto in particolare dal citato articolo 7 - della stretta necessità del trattamento risulta confermato, anche sulla base delle risultanze istruttorie, in ragione della funzionalità di tale sistema rispetto alle attività di identificazione svolte dalle forze di polizia »*, , *Ibidem*, traduit par nous.

232 *« Il trattamento in argomento costituisce, infatti, un mero ausilio all'agire umano, avente lo scopo di velocizzare l'identificazione, da parte dell'operatore di polizia, di un soggetto ricercato della cui immagine facciale si disponga, ferma restando l'esigenza dell'intervento dell'operatore per verificare l'attendibilità dei risultati prodotti dal sistema automatizzato »*, ***Ibidem***, traduit par nous.

233 Garante Per La Protezione Dei Dati Personali, Décision n°8789277 rendue le 15 mars 2018.

de mesure des flux de passagers. Elle a considéré que le traitement de données biométriques est compatible avec le principe de minimisation des données car « les images sont conservées pendant le temps strictement nécessaire à leur codage dans un modèle biométrique, et sans aucun recoupement avec d'autres données d'identification (par exemple, nom et prénom) des personnes concernées ».[234]

Le régulateur italien ne plaide donc pas, à travers ses décisions, pour la création d'un régime juridique spécifique à la reconnaissance faciale. En revanche, il exige que les conditions posées par le droit des données personnelles existant soient respectées.

III. Les cas d'usages

La reconnaissance faciale a été déployée en Italie dans des situations variées. Nous développerons en l'espèce les cas d'usage de la reconnaissance faciale à des fins policières (A) et dans les aéroports (B).

A - Un cas d'usage de la reconnaissance faciale à des fins policières

Le *Sistema Automatico di Riconoscimento Immagini* (ci-après dénommé « SARI ») est un logiciel sophistiqué de reconnaissance faciale utilisé par la police italienne. Le Ministère de l'Intérieur italien a attribué la fourniture du logiciel en janvier 2017 à la société Parsec 3.26 établie à Lecce, qui collabore avec *l'Istituto di Scienze Applicate e Sistemi Intelligenti* pour le développement d'algorithmes de reconnaissance faciale. SARI a deux modes de fonctionnement : Entreprise et Realtime[235].

- *En mode Entreprise*, l'algorithme garantit à la police un système de recherche de l'identité d'un visage dans la base de données *Sistema Automatizzato di Identificazione delle Impronte*. Cette base de données est constituée des visages d'environ 9 millions de personnes, dont 7 millions d'étrangers. Selon une enquête réalisée par *Wired*, il s'agit principalement de migrants arrivant en Italie qui sont tenus de fournir aux autorités leurs empreintes digitales et qui font l'objet d'un signalement photographique[236]. La recherche peut être effectuée à partir d'une image du visage d'un sujet inconnu, d'informations géographiques ou descriptives associées aux images, voire d'une combinaison des deux méthodes. Le logiciel fournit alors une liste d'images classées selon des degrés de similitude[237]. Le régulateur italien a été amené à se positionner sur cet usage en différé lors de la décision n°9040256 du 26 juillet 2018 précédemment citée.

- *En mode Realtime*, le système peut analyser en temps réel les visages des sujets filmés par les caméras, en les comparant à une liste de surveillance. Une fois que le SARI a identifié un visage, il le communique aux agents avec une alerte. Les capacités de reconnaissance se comptent par centaines de milliers de sujets[238]. En l'état de notre connaissance, nous ignorons si une analyse d'impact a été réalisée pour chacun de ses deux modes.

En juillet 2017, l'utilisation du logiciel SARI Entreprise par la Police nationale de Brescia a permis l'identification et l'arrestation de deux cambrioleurs de nationalité géorgienne[239]. Dans ce médiatique cas d'espèce,

234 *« Ciò viene realizzato con modalità tali da minimizzare l´utilizzo dei dati personali, essendo le immagini conservate per gli istanti strettamente necessari alla loro codifica in template biometrico, e senza che sia effettuato alcun incrocio con altri dati identificativi (es. nome e cognome) dei soggetti, con la conseguenza di un trattamento di dati ridotto al minimo »*, *Ibidem*, traduit par nous.

235 G. PACINO, « Come funziona Sari, il sistema di riconoscimento facciale usato dalla Polizia scientifica » [en ligne], *La Repubblica*, 7 septembre 2018, [consulté le 15/01/2020], https://www.repubblica.it/cronaca/2018/09/07/news/come_funziona_sari_il_sistema_di_riconoscimento_facciale_usato_dalla_polizia_scientifica-205804445/?refresh_ce

236 R. ANGIUS, R. COLUCCINI, « Riconoscimento facciale, nel database di Sari quasi 8 schedati su 10 sono stranieri » [en ligne], *Wired*, 03 April 2019, [consulté le 15/01/2020], https://www.wired.it/attualita/tech/2019/04/03/sari-riconoscimento-facciale-stranieri/

237 G. PACINO, « Come funziona Sari, il sistema di riconoscimento facciale usato dalla Polizia scientifica », précédemment cité.

238 *Ibidem.*

239 *Ibidem.*

le traitement a été appliqué, a posteriori, sur des images capturées par une caméra de vidéosurveillance privée[240]. Cette illustration témoigne de la porosité entre l'espace public et l'espace privé dans l'usage de cette technologie à des fins policières.

B - Les cas d'usage de la reconnaissance faciale dans les aéroports

En Italie, la reconnaissance faciale est déployée dans les aéroports à des fins de contrôle aux frontières extérieures (1). Certains aéroports connaissent également des expérimentations de cette technologie à l'embarquement (2).

1. L'installation du dispositif eGates au contrôle aux frontières extérieures

eGates est un dispositif de contrôle automatisé des passeports, mis en place en Italie aux frontières extérieures dans le sens des départs et des arrivées. Ce portail « augmenté » s'appuie sur la reconnaissance faciale ; il vise à accroître la sécurité et diviser par deux le temps d'attente des passagers par rapport à un contrôle traditionnel. Les données biométriques sont extraites de la photographie stockée sur la puce du passeport puis comparées à celles déduites de l'image capturée lors du contrôle. Lorsque la correspondance est établie, le portique s'ouvre afin de laisser passer le passager. A l'inverse, en cas de correspondance erronée, le passager doit se rendre dans un point de contrôle tenu par un opérateur humain.[241]

L'aéroport Roma Fiumicino Leonardo da Vinci a été le premier à accueillir cette solution, en 2014[242]. Ces portiques ont ensuite été installés dans plusieurs aéroports italiens : l'aéroport Roma Ciampino[243], l'aéroport Capodichino de Naples[244], l'aéroport Guglielmo Marconi de Bologne[245], l'aéroport Marco Polo de Venise[246], l'aéroport de Cagliari[247], l'aéroport Antonio Canova[248] et l'aéroport de Milan Malpensa[249]. La société Toscani Aeroporti S.p.A a également pris la décision d'installer ces portiques dans les aéroports de Pise et de Florence en 2018[250].

Ces dispositifs eGates sont fournis aux aéroports par différentes entreprises. A Trévise[251] et à Venise[252], les portails implémentant une solution de reconnaissance faciale ont été fournis par Naitec, une société établie

240 Polizia di Stato, *« Brescia : ladri d'appartamento scoperti grazie al riconoscimento facciale »*, [en ligne], 07/09/2018, [consulté le 10/03/2020] : https://www.poliziadistato.it/articolo/135b92536bb3957899899171

241 Aeroporti di Roma, « E-gates » [en ligne] [consulté le 10/03/2020], http://www.adr.it/fr/web/aeroporti-di-roma-en-/e-gates

242 *Ibidem*

243 *Ibidem*

244 Passenger Self Service, « Naples Introduces ABC EGates For EU Passengers » [en ligne], *Passenger Self Service*, 19 janvier

245 Passenger Self Service, « Bologna Airport Gets ABC e-Gates » [en ligne], *Passenger Self Service*, 03 Février 2017 [consulté le

246 Venezia Airport, « Notice on e-Gates » [en ligne], *Venezia Airport*, [consulté le 10/03/2020], https://www.veneziaairport.

247 Cagliari Airport Sogaer, « L'aeroporto attiva gli e-Gate » [en ligne], *Cagliari Airport Sogaer*, 29 mai 2019 [consulté le

248 Treviso Airport, « Notice on e-Gates » [en ligne], *Treviso Airport*, [consulté le 10/03/2020], https://www.trevisoairport.it/

249 M. Canorro, *« Malpensa, al via i primi e-gates : controlli biometrici sui passeggeri »* [en ligne], *Corriere Comunicazioni*, 09 Juillet 2015 [consulté le 10/03/2020] : https://www.corrierecomunicazioni.it/digital-economy/malpensa-al-via-i-primi-e-gates-

250 Teleborsa, « Nel 2018 sette e-Gates negli aeroporti toscani » [en ligne], 05 février 2018, *Teleborsa*, [consulté le 10/03/2020], https://www.teleborsa.it/News/2018/02/05/nel-2018-sette-e-gates-negli-aeroporti-toscani-131.html#.XmkA-aclBQL

251 Naitec, Page Twitter de Naitec [en ligne], 02 août 2018, 4:12 p.m [consulté le 10/03/2020] : https://twitter.com/NaitecSolutions/status/1025022425971535873?s=20

252 Naitec, Page Twitter de Naitec [en ligne], 06 juillet 2018, 10:24 a.m [consulté le 10/03/2020] : https://twitter.com/NaitecSolutions/status/1015149571113091075

en Vénétie. Les aéroports de Rome Fiumicino[253], de Naples[254] et de Bologne[255] ont été dotés de portiques conçus par la Société internationale de télécommunications aéronautique, une coopérative genevoise. Enfin, ceux de l'aéroport de Milan Malpensa ont été élaborés par un consortium réunissant NTT Data, Indra, Secunet et Studio Fra[256] . En l'état de notre connaissance, nous ignorons si une analyse d'impact a été réalisée en amont de leur installation.

2. L'expérimentation de la reconnaissance faciale à l'embarquement

a) L'aéroport Roma Fiumicino

L'aéroport Roma Fiumicino est le premier aéroport d'Italie à expérimenter une procédure d'embarquement reposant sur la reconnaissance faciale pour les vols à destination d'Amsterdam assurés par la compagnie aérienne KLM. Ce projet pilote est le fruit d'un partenariat avec la société portugaise Vision Box - soutenu par la police nationale et l'autorité italienne de l'aviation civile - pendant une durée de six mois, jusqu'au 31 mars 2020[257]. Cette expérimentation entend faciliter la vie des usagers en les dispensant de présenter divers documents à chaque point de contrôle. Lors de l'enregistrement, un appareil IoT collecte leurs données biométriques ainsi que leurs données personnelles contenues dans leur passeport et leur carte d'embarquement[258]. Des caméras sont placées dans des zones spécifiques de l'aéroport et détectent les caractéristiques biométriques des visages des passagers aux différents points de passage pour assurer leur identification. Les données sont ensuite effacées des serveurs de l'aéroport dans l'heure qui suit le décollage[259]. Une nouvelle fois, nous n'avons pas eu connaissance de la réalisation d'une analyse d'impact préalable.

b) L'aéroport Milano Linate

L'aéroport Milano Linate a également mis en place, à titre expérimental, une procédure d'embarquement s'appuyant sur la reconnaissance faciale. Ce projet pilote durera jusqu'au 31 décembre 2020 sur les vols à destination de Rome Fiumicino assurés par la compagnie aérienne Alitalia[260]. Deux régimes de conservation des données sont prévus par la politique de protection de la vie privée de la Società per azioni Esercizi Aeroportuali, la société en charge de la gestion de l'aéroport. Les données personnelles relatives au passeport ainsi que les données biométriques sont cryptées et conservées pendant une période allant de 24 heures jusqu'au 31 décembre 2020 selon le consentement de la personne concernée. Les données personnelles uniquement liées à la carte d'embarquement sont supprimées 48 heures après le décollage[261]. En l'état de notre connaissance, nous ignorons si cette expérimentation a donné lieu à une analyse d'impact.

---

253 Passenger Self Service, « ABC EGates Installed At Rome Fiumicino » [en ligne], 30 Octobre 2014, *Passenger Self Service* [consulté le 10/03/2020], https://www.passengerselfservice.com/2014/10/8-abc-egates-installed-at-rome-fiumicino/

254 Passenger Self Service, « Naples Introduces ABC EGates For EU Passengers » [en ligne], *Passenger Self Service*, 19 janvier 2016 [consulté le 10/03/2020], http://www.passengerselfservice.com/2016/01/naples-introduces-abc-egates-for-eu-passengers/

255 Passenger Self Service, « Bologna Airport Gets ABC e-Gates » [en ligne], *Passenger Self Service,* 03 Février 2017 [consulté le 10/03/2020], http://www.passengerselfservice.com/2017/02/bologna-airport-gets-abc-e-gates/, http://www.passengerself-service.com/2017/02/bologna-airport-gets-abc-e-gates/

256 M. canorro, *« Malpensa, al via i primi e-gates : controlli biometrici sui passeggeri »,* précédemment cité.

257 Turismo Roma, « Il futuro sbarca a Fiumicino: check-in con riconoscimento facciale e liquidi in valigia » [en ligne], *Turismo Roma,* [consulté le 10 mars 2020], http://www.turismoroma.it/it/notizie/il-futuro-sbarca-fiumicino-check-con-riconoscimento-facciale-e-liquidi-valigia

258 Vision Box, « Rome, Italy : Vision-Box Seamless Flow OneID Trial At Fiumicino Aeroporti di Roma, Italy » [en ligne], *Vision Box*, 23 janvier 2020 [consulté le 10/03/2020], https://www.vision-box.com/pressroom/press-releases/seamless-flow-trial-fiumicino-aeroporti-di-roma

259 Aeroporto Di Roma, « Il controllo biometrico » [en ligne][consulté le 10/03/2020], http://www.adr.it/fr/controllo-biometrico

260 Milano Linate Airport, « Face Boarding » [en ligne] [consulté le 10/03/2020], https://www.milanolinate-airport.com/en/flights/face-boarding

261 Milano Linate Airport, « Privacy Policy » [en ligne] [consulté le 10/03/2020], https://www.milanolinate-airport.com/assets/4/AbstractPage/239/C_4_AbstractPage_741_2_downloadFile.pdf

BIBLIOGRAPHIE

I . Législation

- Decreto Legislativo, 18 mai 2018,

  https://www.gazzettaufficiale.it/eli/id/2018/05/24/18G00080/sg

II. Prise de position des autorités régulatrices de la protection des données

- Garante Per la Protezione Dei Dati « Personali, Sistema automatico di ricerca dell'identità di un volto », 26 juillet 2018, n°9040256, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9040256
- Garante Per la Protezione Dei Dati « Verifica preliminare. Sistema di rilevazione delle immagini dotato di un software che permette il riconoscimento della persona (morfologia del volto) » - 15 marzo 2018 [8789277], https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/8789277

III. Presse numérique

- Aeroporti di Roma, « E-gates » [en ligne] [consulté le 10/03/2020], http://www.adr.it/fr/web/aeroporti-di-roma-en-/e-gates
- Aeroporto Di Roma, « Il controllo biometrico » [en ligne][consulté le 10/03/2020], http://www.adr.it/fr/controllo-biometrico
- Angius R and Coluccini R., « Riconoscimento facciale, nel database di Sari quasi 8 schedati su 10 sono stranieri » [en ligne], *Wired*, 3 Avril 2019, [consulté le 15/01/2020], https://www.wired.it/attualita/tech/2019/04/03/sari-riconoscimento-facciale-stranieri/
- Cagliari Airport Sogaer, « L'aeroporto attiva gli e-Gate » [en ligne], *Cagliari Airport Sogaer*, 29 mai 2019 [consulté le 10/03/2020], http://www.sogaer.it/it/sala-stampa/laeroporto-attiva-gli-e-gate
- Cannoro M., « Malpensa, al via i primi e-gates : controlli biometrici sui passeggeri » [en ligne], *Corriere Comunicazioni,* 09 Juillet 2015 [consulté le 10/03/2020], https://www.corrierecomunicazioni.it/digital-economy/malpensa-al-via-i-primi-e-gates-controlli-biometrici-sui-passeggeri/
- Milano Linate Airport, « Face Boarding » [en ligne] [consulté le 10/03/2020], https://www.milanolinate-airport.com/en/flights/face-boarding
- Milano Linate Airport, « Privacy Policy » [en ligne] [consulté le 10/03/2020], https://www.milanolinate-airport.com/assets/4/AbstractPage/239/C_4_AbstractPage_741_2_downloadFile.pdf
- Naitec, Page Twitter de Naitec [en ligne], 06 juillet 2018, 10:24 a.m [consulté le 10/03/2020], https://twitter.com/NaitecSolutions/status/1015149571113091075
- Naitec, Page Twitter de Naitec [en ligne], 02 août 2018, 4:12 p.m [consulté le 10/03/2020], https://twitter.com/NaitecSolutions/status/1025022425971535873?s=20
- Pacino G., « Come funziona Sari, il sistema di riconoscimento facciale usato dalla Polizia scientifica » [en ligne], *La Repubblica*, 7 septembre 2018, [consulté le 15/01/2020], https://www.repubblica.it/cronaca/2018/09/07/news/come_funziona_sari_il_sistema_di_riconoscimento_facciale_usato_dalla_polizia_scientifica-205804445/?refresh_ce
- Passenger Self Service, « ABC EGates Installed At Rome Fiumicino » [en ligne], 30 Octobre 2014, *Passenger Self Service* [consulté le 10/03/2020], https://www.passengerselfservice.com/2014/10/8-abc-egates-installed-at-rome-fiumicino/

- Passenger Self Service, « Naples Introduces ABC EGates For EU Passengers » [en ligne], *Passenger Self Service*, 19 janvier 2016 [consulté le 10/03/2020], http://www.passengerselfservice.com/2016/01/naples-introduces-abc-egates-for-eu-passengers/
- Passenger Self Service, « Bologna Airport Gets ABC e-Gates » [en ligne], *Passenger Self Service*, 03 Février 2017 [consulté le 10/03/2020], http://www.passengerselfservice.com/2017/02/bologna-airport-gets-abc-e-gates/
- Polizia di Stato, « Brescia : ladri d'appartamento scoperti grazie al riconoscimento facciale » [en ligne], *Polizia di Stato*, 07 septembre 2018 [consulté le 10/03/2020], https://www.poliziadistato.it/articolo/135b92536bb3957899899171
- Teleborsa, « Nel 2018 sette e-Gates negli aeroporti toscani » [en ligne], 05 février 2018, *Teleborsa,* [consulté le 10/03/2020], https://www.teleborsa.it/News/2018/02/05/nel-2018-sette-e-gates-negli-aeroporti-toscani-131.html#.XmkA-aclBQL
- Treviso Airport, « Notice on e-Gates » [en ligne], *Treviso Airport*, [consulté le 10/03/2020], https://www.trevisoairport.it/en/news/169/notice-on-e-gates.html
- Turismo Roma, « Il futuro sbarca a Fiumicino: check-in con riconoscimento facciale e liquidi in valigia » [en ligne], *Turismo Roma,* [consulté le 10/03/2020], http://www.turismoroma.it/it/notizie/il-futuro-sbarca-fiumicino-check-con-riconoscimento-facciale-e-liquidi-valigia
- Venezia Airport, « Notice on e-Gates » [en ligne], *Venezia Airport*, [consulté le 10/03/2020], https://www.veneziaairport.it/en/news/169/notice-on-e-gates.html
- Vision Box, « Rome, Italy : Vision-Box Seamless Flow OneID Trial At Fiumicino Aeroporti di Roma, Italy » [en ligne], *Vision Box*, 23 janvier 2020 [consulté le 10/03/2020], https://www.vision-box.com/pressroom/press-releases/seamless-flow-trial-fiumicino-aeroporti-di-roma

Pays-Bas

I. Législation

Aux Pays-Bas, il n'existe pas de législation spécifique encadrant l'utilisation de la reconnaissance faciale. Cependant, plusieurs textes nationaux et généraux posent les premiers jalons d'un encadrement légal de la technologie. L'*Uitvoeringswet Algemene verordening gegevensbescherming* du 16 mai 2018 implémente le RGPD dans le droit interne[262]. Le *Wet politiegegevens* du 21 juillet 2007[263] et le *Wet justitiële en strafvorderlijke gegevens* du 7 novembre 2002[264] - tous deux révisés le 17 octobre 2018 - , transposent la directive Police Justice en droit néerlandais[265]. En tout état de cause, l'usage de la reconnaissance faciale dans l'espace public implique un traitement de données personnelles et doit donc se conformer à ces textes.

Selon *Algorithm Watch*[266], *la police néerlandaise utilise la reconnaissance faciale et peut accéder à une base de données des visages de plus de 1,3 million de personnes*[267]. Il s'agirait de personnes condamnées ou suspectées d'avoir commis un crime punissable d'au moins un an de prison[268]. Le régime de conservation des données associé à cette base est différent selon la culpabilité ou non de la personne concernée. Lorsque les suspects sont reconnus innocents, leurs données doivent être effacées ; les données des personnes condamnées sont conservées entre 20 et 80 ans selon le type de délit[269]. Par ailleurs, les visages des suspects figurant sur cette base de données peuvent être comparés à ceux des demandeurs d'asile, mais une autorisation du ministère public est requise[270].

II. Position de l'autorité de protection des données

La mise en place de la reconnaissance faciale aux Pays-Bas a conduit l'autorité néerlandaise de protection des données à se prononcer sur le sujet. Cette prise de position s'exprime à travers des lignes directrices applicables à la surveillance par caméras (A) et des courriers adressés à des acteurs privés (B).

A. Les lignes directrices applicables à la surveillance par caméras

En 2016, l'agence néerlandaise de protection des données a publié des lignes directrices applicables à la surveillance par caméras[271]. L'usage de la reconnaissance faciale dans l'espace public impliquant l'installation de caméras pour capturer l'image faciale des individus, la mise en œuvre de cette technologie nécessite dès lors de s'y conformer. À ce titre, l'autorité de contrôle s'est prononcée sur le régime juridique applicable à la reconnaissance faciale. Sa position apparaît quelque peu ambiguë. Alors même que « l'utilisation de caméras

262 Uitvoeringswet Algemene verordening gegevensbescherming, 16 mai 2018 : https://wetten.overheid.nl/BWBR0040940/2020-01-01

263 Wet politiegegevens, 21 juillet 2007 : https://wetten.overheid.nl/BWBR0022463/2020-01-01

264 Wet justitiële en strafvorderlijke gegevens, 7 novembre 2002 : https://wetten.overheid.nl/BWBR0014194/2020-01-01

265 Wet van 17 oktober 2018 tot wijziging van de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens ter implementatie van Europese regelgeving over de verwerking van persoonsgegevens met het oog op de voorkoming, het onderzoek, de opsporing en vervolging van strafbare feiten of de tenuitvoerlegging van straffen : https://zoek.officielebekendmakingen.nl/stb-2018-401.html

266 N. KAYSER-BRIL, "At least 10 police forces use face recognition in the EU, AlgorithmWatch reveals" [en ligne], *Algorithme watch*, 11 décembre 2019, [consulté le 13/01/2020], https://algorithmwatch.org/en/story/face-recognition-police-europe/

267 NEXT INPACT, « L'Europe généralise la reconnaissance faciale policière » [en ligne], *INpact*, 12 décembre 2019, [consulté le 28/01/2020], https://www.nextinpact.com/brief/l-europe-generalise-la-reconnaissance-faciale-policiere-10643.htm

268 Selon les propos de la police, rapportés par la presse. J. SCHELLEVIS, « POLITIE GAAT VERDACHTEN OPSPOREN MET GEZICHTSHERKENNING » [EN LIGNE], *NOS*, 16 DÉCEMBRE 2016, [CONSULTÉ LE 13 MARS 2020] : HTTPS://NOS.NL/ARTIKEL/2148598-POLITIE-GAAT-VERDACHTEN-OPSPOREN-MET-GEZICHTSHERKENNING.HTML

269 J. SCHELLEVIS, précédemment cité

270 J. SCHELLEVIS, précédemment cité

271 COLLEGE BESCHERMING PERSOONSGEGEVENS, *Beleidsregels cameratoezicht*, 2016, https://wetten.overheid.nl/BWBR0037591/2016-02-02

intelligentes n'a, selon elle, aucune influence sur les réglementations légales applicables dans une situation spécifique »[272], elle fait état d'un risque accru d'atteinte à la vie privée: « les caméras avec reconnaissance faciale peuvent automatiquement tracer, suivre et profiler des personnes, ce qui n'est pas possible avec des caméras ordinaires »[273].

B. Les courriers adressés à des acteurs privés

Dans un courrier du 3 février 2004, l'autorité néerlandaise de protection des données (Autoriteit Persoonsgegevens) fut amenée à se positionner sur la demande d'une organisation faîtière. Pour sécuriser ses évènements publics, l'organisation souhaitait s'appuyer sur un système associant l'utilisation d'une carte à puce à de la reconnaissance faciale, pour vérifier l'identité des détenteurs de ladite carte. L'autorité de contrôle indiqua à cette occasion qu'elle n'était pas opposée à l'utilisation de la biométrie dans le cadre d'un contrôle d'accès, car cela permettait d'éviter un traitement de données personnelles inutile[274]. Elle releva cependant que le concept envisagé présentait un lien étroit entre le contrôle d'accès et l'identification. L'autorité de contrôle nuance toutefois au point 6.1.2[275] de ce courrier que « la capture du modèle biométrique de tous les visiteurs d'un évènement se révèle souvent être une mesure disproportionnée par rapport à la cible d'identification ». Dès lors, les données biométriques d'un grand nombre d'individus ne peuvent pas, en principe, être collectées pour s'assurer de l'identité d'une seule personne.

Plus récemment, le régulateur néerlandais a été amené à se prononcer sur l'utilisation de la reconnaissance faciale par des annonceurs publicitaires. Dans un courrier du 25 juin 2018, il indiqua que ces derniers pouvaient utiliser des caméras dans des panneaux d'affichage numériques sur l'espace public afin d'afficher des publicités ciblées aux passants. Ces caméras peuvent être équipées de logiciel de reconnaissance faciale et d'analyse permettant de tirer des conclusions sur le sexe, l'âge et l'humeur des passants[276].

III. Cas d'usage

Les expérimentations et usages de la reconnaissance faciale aux Pays-Bas se concentrent principalement sur trois secteurs : la police (A), les zones commerciales (B) et les aéroports (C).

A - Un usage policier de la reconnaissance faciale

1) Le système de reconnaissance faciale « MorphoBIS » au service de la police nationale

Depuis 2016, la police nationale des Pays-Bas utilise un dispositif de reconnaissance faciale[277] fourni par la société *« Safran Identity & Security »*[278]. Ce dispositif a été adopté par le Centre national de la police judiciaire. Il permet de rechercher, comparer et analyser des photos et images afin de trouver ou identifier un

---

272 *Ibidem.*, point 5.3, https://wetten.overheid.nl/BWBR0037591/2016-02-02#Circulaire.divisie : ***« geldt ook hier dat de inzet van slimme camera's geen invloed heeft op de wettelijke regelingen die in een concrete situatie van toepassing zijn »,*** traduit par nous.

273 *Ibidem* point 5.3 : « Camera's met gezichtsherkenning kunnen bijvoorbeeld personen op geautomatiseerde wijze traceren, volgen en profileren, hetgeen met reguliere camera's niet mogelijk is », traduit par nous.

274 *Autoriteit Persoonsgegevens,* **« Vragen over inzet gezichtsherkenning »**, courrier du 3 février 2004, point 5.1.2, https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/uit/z2003-1529.pdf?fbclid=IwAR1q0DeAsRsAf3iEuAunB9x1GFRIY-

275 *Autoriteit Persoonsgegevens,* **« Vragen over inzet gezichtsherkenning »**, courrier du 3 février 2004, point 6.1.2 : ***«het vastleggen van biometrische templates van alle bezoekers van een evenement al gauw disproportioneel ten opzichte van het***

276 *Autoriteit Persoonsgegevens,* « Normenkader digitale billboards », courrier du 25 juin 2018, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/brief_branche_normkader_digitale_billboards.pdf?fbclid=IwAR1Q2m-6MYv_EU0qTN-g84inF6rG1KdZePPgOIul6gWYnOwrCfY4oWpNw-wM

277 J. Schellevis, "Politie gaat verdachten opsporen met gezichtsherkenning" [en ligne], *Nos*, 16 décembre 2016, [consulté le 14/01/2020], https://nos.nl/artikel/2148598-politie-gaat-verdachten-opsporen-met-gezichtsherkenning.html

278 Safran, « La police nationale des Pays-Bas choisit le système de reconnaissance faciale de Safran Identity & Security » [en ligne], *Safran Groupe*, [consulté le 28/01/2020], https://www.safran-group.com/fr/media/la-police-nationale-des-pays-bas-

individu. À cet effet, le système de reconnaissance faciale « *MorphoBIS* »[279] dispose de deux fonctionnalités : l'option expert qui « *propose des fonctions avancées d'investigation avec des outils d'analyse et de comparaison d'images présentes dans les bases de données de la police* » ; la seconde, l'option détective permet « *de créer des séries de portraits pour les montrer aux témoins et accéder les enquêtes* ».

Notons qu'avant son adoption, la société Safran fournissait des solutions biométriques permettant à la police néerlandaise de diligenter des recherches similaires à partir d'empreintes digitales palmaires.

2) L'usage du système de reconnaissance faciale « Catch » pour la police

Les forces de police des Pays-Bas sont également munies du système dit « Catch[280] » sur leurs caméras. Le responsable de sa mise en œuvre est le directeur du Centre de biométrie du Service national de coopération opérationnelle, John Riemen[281]. Ce logiciel permet d'établir des correspondances, au départ de photo transmise, dans le cadre de recherche ; il ne peut pas analyser les images en temps réel.

Les policiers municipaux utilisent parallèlement des « *bodycams* » - caméras corporelles embarquées[282]. Dans ce cas de figure, la caméra fonctionne en temps réel. Elle compare les visages à une base de données locale et avertit l'agent d'une correspondance. Le policier vérifie dans un second temps l'exactitude de l'alerte afin de prendre les mesures adéquates à la situation. Cette pratique a recours au nouveau réseau de communication Tec4se[283], lequel connecte les réseaux, collecte et regroupe les données de la police, des pompiers et des images caméras afin de permettre un meilleur déploiement des forces de l'ordre.

Le dispositif néerlandais devrait inspirer de nouvelles expérimentations. La Belgique envisage ainsi de s'en inspirer pour ses propres unités[284].

B - Le cas particulier de la surveillance des zones commerciales

Afin de lutter contre le vol à l'étalage, la grande surface alimentaire *Jumbo Ten Brink Fooda,* présentée comme le « magasin le plus sûr des Pays-Bas[285] », a mis en place, en mars 2017, un dispositif de reconnaissance faciale dans ses établissements. Le fondateur explique que « dès qu'un voleur identifié essaye d'entrer dans le magasin, une alarme interne est déclenchée et nous pouvons prendre les mesures nécessaires »[286]. L'enseigne a mis en place 80 caméras afin de lutter contre le vol à l'étalage par le biais de grands sacs de course. Elle recourt au système de reconnaissance faciale vendu par Panasonic, qui s'appuie sur un système d'apprentissage automatique pour obtenir le résultat le plus optimal et améliorer les performances du système. Ce dispositif offrirait des résultats efficaces en « détectant les visages même lorsqu'ils sont inclinés » (...) présentant "un taux d'exactitude de 90% dans le cas de visages partiellement cachés par des lunettes de soleil ou des masques » ; il reconnaîtrait également des visages à partir de photographies vieilles de 10 ans[287]. L'application serait également mobilisée en temps réel, en cas de vol : une vingtaine de caméras stockent les images sur

---

279 IDEMIA, « La police nationale des Pays-Bas choisit le système de reconnaissance faciale de Safran Identity & Security » [en ligne], *Idemia*, 16 mars 2017, [consulté le 28/01/2020], https://www.idemia.com/fr/press-release/la-police-nationale-des-pays-bas-choisit-le-systeme-de-reconnaissance-faciale-de-safran-identity-security-2017-03-16

280 W. VAN GAAL, « RECONNAISSANCE FACIALE DANS LES RUES HOLLANDAISES: FAUT-IL LE VOULOIR? » [EN LIGNE], *VICE*, 18 JUILLET 2019, [CONSULTÉ LE 14/01/2020] HTTPS://WWW.VICE.COM/NL/ARTICLE/8XZYDZ/GEZICHTSHERKENNING-OP-DE-NEDERLANDSE-STRATEN-MOETEN-WE-DAT-WILLEN

281 *Ibidem,* Dienst Landelijke Operationele Samenwerking, traduit par nous.

282 Selon Luuk Spreeuwers, professeur de biométrie à l'Université de Twente, conseil auprès de la police sur les questions de reconnaissance faciale. Son logiciel est utilisé par les institutions privées avec lesquelles la police néerlandaise collabore, *Ibidem.*

283 Tec4se est un nouveau système de réseau innovant dans le domaine de la sécurité qui relie les informations de différents services et contribue ainsi à optimiser la prise de décision : https://www.regiotwente.nl/over-regio-twente/pers-en-media/nieuws/731-nieuw-communicatienetwerk-tec4se-ondersteunt-veiligheids-en-hulpverleningsdiensten-bij-inzet

284 Voy. *Supra.*

285 M. ROSSIGNOL « UNE ENSEIGNE NÉERLANDAISE RÉCOMPENSÉE POUR L'EXCELLENCE DE SA POLITIQUE DE SÉCURITÉ », *PRÉVENTICA*, 6 MARS 2019, HTTPS://WWW.PREVENTICA.COM/ACTU-ENBREF-MAGASIN-CONTROLE-ACCES-RECONNAISSANCE-FACIALE-060319.PHP

286 *Ibidem.*

287 *Ibidem.*

une base de données pour les comparer à une base de 30 000 visages de référence. La base de données est constituée des personnes ayant été surprises en flagrant délit de vol par les caméras du magasin.

C - Le cas de l'expérience à l'aéroport d'Amsterdam-Schiphol

Les Pays-Bas sont en pleine réflexion sur un nouveau dispositif d'identification biométrique permettant aux passagers de prendre leur vol sans leur passeport[288]. Toutefois, les failles de la technologie mises en lumière par des expériences passées à l'aéroport d'Amsterdam-Schiphol alimentent encore les réticences[289].

288 M. LADIRAY, « BIOMÉTRIE, MOBILE, AUTOMATISATION : L'AÉROPORT SERA CONNECTÉ OU NE SERA PAS » [EN LIGNE], *TOM.TRAVEL*, 8 NOVEMBRE 2019, [CONSULTÉ LE 15/01/2020] HTTPS://WWW.TOM.TRAVEL/2019/11/08/BIOMETRIE-MOBILE-AUTOMATISATION-AEROPORT-SERA-CONNECTE-OU-NE-SERA-PAS/

289 Des chercheurs rattachés à la société *Kneron* ont démontré qu'il était aisé de tromper ces systèmes à l'aide de masque 3D, de photographies imprimées ou numériques. Munis d'une photo d'une autre personne sur son téléphone, un individu a pu se faire passer pour une autre personne lors du contrôle : tromper le système ne requiert pas de compétences techniques approfondies. A. LE DENN, « Des systèmes de reconnaissance faciale auraient été trompés par des masques et photos » [en ligne], *L'Usine digitale*, 16 décembre 2019, [consulté le 15/01/2020], https://www.usine-digitale.fr/article/des-systemes-de-reconnaissance-faciale-auraient-ete-trompes-par-des-masques-et-photos.N913919

BIBLIOGRAPHIE

I. Législation

- Loi du 16 mai 2018 d'exécution du règlement général sur la protection des données, https://wetten.overheid.nl/BWBR0040940/2020-01-01
- Loi du 21 juillet 2007 sur les données de la police, https://wetten.overheid.nl/BWBR0022463/2020-01-01
- Loi du 7 novembre 2002 sur le casier judiciaire et criminel, https://wetten.overheid.nl/BWBR0014194/2020-01-01
- Loi du 3 juillet 2013 sur l'enregistrement des personnes, https://wetten.overheid.nl/BWBR0033715/2019-02-03
- Règles politiques pour la surveillance par caméra, Autorité néerlandaise de protection des données, https://wetten.overheid.nl/BWBR0037591/2016-02-02

II. Prise de position des autorités régulatrices de la protection des données

- https://autoriteitpersoonsgegevens.nl/en
- https://autoriteitpersoonsgegevens.nl/nl/over-privacy/wetten/algemene-verordening-gegevensbescherming-avg

III. Presse numérique

- Idemia, « La police nationale des Pays-Bas choisit le système de reconnaissance faciale de Safran Identity & Security » [en ligne], *Idemia*, 16 mars 2017, [consulté le 28/01/2020], https://www.idemia.com/fr/press-release/la-police-nationale-des-pays-bas-choisit-le-systeme-de-reconnaissance-faciale-de-safran-identity-security-2017-03-16
- Les Echos, « Uber condamné aux Pays-Bas et au Royaume-Uni après un piratage de données » [en ligne], *Les Echos*, 28 novembre 2018, [consulté le 15/01/2020], https://www.lesechos.fr/industrie-services/tourisme-transport/uber-condamne-aux-pays-bas-et-au-royaume-uni-apres-un-piratage-de-donnees-150900
- Nicolas KAYSER-BRIL, "At least 10 police forces use face recognition in the EU, AlgorithmWatch reveals" [en ligne], *Algorithme watch*, 11 décembre 2019, [consulté le 13/01/2020], https://algorithmwatch.org/en/story/face-recognition-police-europe/
- Margot LADIRAY, « Biométrie, mobile, automatisation : l'aéroport sera connecté ou ne sera pas » [en ligne], *TOM.travel*, 8 novembre 2019, [consulté le 15/01/2020] , https://www.tom.travel/2019/11/08/biometrie-mobile-automatisation-aeroport-sera-connecte-ou-ne-sera-pas/
- Arthur LE DENN, « Des systèmes de reconnaissance faciale auraient été trompés par des masques et photos » [en ligne], *L'Usine digitale*, 16 décembre 2019, [consulté le 15/01/2020], https://www.usine-digitale.fr/article/des-systemes-de-reconnaissance-faciale-auraient-ete-trompes-par-des-masques-et-photos.N913919
- Next inpact, « L'Europe généralise la reconnaissance faciale policière » [en ligne], *INpact*, 12 décembre 2019, [consulté le 28/01/2020], https://www.nextinpact.com/brief/l-europe-generalise-la-reconnaissance-faciale-policiere-10643.htm

- Magali ROSSIGNOL, « Une enseigne néerlandaise récompensée pour l'excellence de sa politique de sécurité », *Préventica*, 6 mars 2019, https://www.preventica.com/actu-enbref-magasin-controle-acces-reconnaissance-faciale-060319.php

- Safran, « La police nationale des Pays-Bas choisit le système de reconnaissance faciale de Safran Identity & Security » [en ligne], *Safran Groupe*, [consulté le 28/01/2020], https://www.safran-group.com/fr/media/la-police-nationale-des-pays-bas-choisit-le-systeme-de-reconnaissance-faciale-de-safran-identity-security-20170316

- Joost SCHELLEVIS, "Politie gaat verdachten opsporen met gezichtsherkenning" [en ligne], *Nos*, 16 décembre 2016, [consulté le 14/01/2020], https://nos.nl/artikel/2148598-politie-gaat-verdachten-opsporen-met-gezichtsherkenning.html

- Wester VAN GAAL, « Reconnaissance faciale dans les rues hollandaises: faut-il le vouloir? » [en ligne], *Vice*, 18 juillet 2019, [consulté le 14/01/2020], https://www.vice.com/nl/article/8xzydz/gezichtsherkenning-op-de-nederlandse-straten-moeten-we-dat-willen

République Tchèque

I. Législation

En l'absence de législation spécifique sur la reconnaissance faciale, c'est principalement le droit de la protection des données qui encadre les usages de la reconnaissance faciale.

Le 12 mars 2019, la République tchèque a approuvé une loi intégrant les dispositions du RGPD[290]. La chambre des députés a adopté la version finale de la loi sur le traitement des données abrogeant la précédente loi n°101/2000 Coll. (Protection des Données personnelles) qui était inapplicable à partir du jour de l'entrée en vigueur du RGPD. Cette loi régit également la compétence de l'Office pour la protection des données personnelles et le traitement des données personnelles au moment d'assurer la défense et la sécurité de la République tchèque. Elle est entrée en vigueur le 24 avril 2019.

Parallèlement à la loi sur le traitement des données, des modifications mineures ont été apportées à des dizaines de lois concernant le traitement des données à caractère personnel. En effet, dans un effort d'harmonisation, quelques dérogations sont à relever.

La détermination du caractère adéquat du traitement comprend une analyse de l'éventail des données à caractère personnel utilisées à ces fins, en particulier si les catégories spéciales de données à caractère personnel et les données relatives aux condamnations et infractions pénales doivent être traitées.

Enfin, mentionnons le fait que la République tchèque a choisi d'exempter totalement ses autorités publiques et ses organismes publics de sanctions administratives. Il ne pèse donc pas de menaces coercitives en cas de dérive d'utilisation de la technologie de reconnaissance faciale.

II. Position de l'Office pour la protection des données personnelles

L'Office pour la protection des données personnelles tchèque (Úřad pro ochranu osobních údajů) a publié des lignes directrices s'agissant de la collecte des données au moyen des dispositifs de vidéosurveillance. Il y met en garde contre les risques et dangers que l'usage de la reconnaissance faciale fait peser sur les droits des personnes concernées. Il rappelle notamment la nécessité des responsables de traitement à procéder à des analyses d'impact, tout en cherchant à avoir recours à des moyens moins intrusifs pour atteindre la finalité légitime du traitement.

La qualification des données biométriques retenue est celle donnée par le RGPD[291].

L'utilisation de la vidéosurveillance, y compris la fonctionnalité de reconnaissance biométrique, installée par des entités privées à leurs propres fins (marketing, statistiques, sécurité) est permise sous réserve d'obtenir le consentement explicite de toutes les personnes concernées.

III. Cas d'usage

Nous avons recensé trois cas d'usage : le recours à la technologie sur un chantier, qui a appelé une prise de position du régulateur (A), et au sein des stades (B) et à l'aéroport de Prague. Nous n'avons pas couvert ce troisième cas, faute d'informations suffisantes.

---

290 "Act of 12 March 2019 on personal data processing" (Act No. 110/2019 Coll.) entré en vigueur le 24 avril 2019 https://www.uoou.cz/en/assets/File.ashx?id_org=200156&id_dokumenty=1837

291 A savoir : sont qualifiées comme telles les données dont le traitement permet « *d'identifier de manière unique une personne physique* »

A - Entreprise de construction

Une entreprise spécialisée dans le secteur de la construction a fait usage de la solution de reconnaissance Face ID dans le but d'identifier les salariés présents sur le chantier[292]. Le dispositif utilisé permettait d'enregistrer l'heure d'arrivée et de départ des salariés par le biais d'un système de reconnaissance faciale. Le système utilisé fonctionnait grâce à un système d'identité numérique, concrètement un gabarit biométrique des salariés était enregistré localement sur un terminal à l'intérieur du bâtiment via une application spécifique. À chaque passage d'un salarié par le portique de reconnaissance faciale, la photo prise par le portique est comparée au gabarit de la personne stockée en interne dans le but d'authentifier son identité et de permettre ainsi d'établir son heure d'entrée et de sortie des lieux.

Position de l'Office pour la protection des données personnelles tchèque. En l'espèce, l'autorité de contrôle a considéré que l'utilisation de Face ID était justifiée et permettait à l'entreprise de BTP, responsable du traitement, de respecter ses obligations légales en matière de sécurité au travail conformément à l'article 316(b) du Code du Travail[293]. L'entité inspectée était en mesure de faire la démonstration que le traitement des données biométriques était nécessaire pour assurer la protection sur ce chantier et qu'elle ne disposait pas d'autres moyens, moins intrusifs pour y parvenir[294]. L'office souligna que sa décision n'avait pas une portée générale[295].

En réponse à cette décision, le législateur tchèque a manifesté la volonté d'encadrer les dispositifs biométriques de surveillance des employés au sein du Code du Travail. L'Office a ainsi eu l'occasion de se prononcer sur le projet d'adaptation des dispositions du Code[296]. Son avis est beaucoup plus réservé : le traitement des données biométriques pour vérifier l'accès et la présence des salariés sur leur lieu de travail doit être exclu[297]. Il critique également le régime de consentement par les employés, qui ne peut être libre et éclairé dans le cadre de la relation employeur-employé. Il rappelle en ce sens - et, conformément aux articles 4 et 7 du RGPD, -que la révocation du consentement par le salarié est une condition sine qua non au traitement de données biométriques.

B - L'usage de la technologie dans les stades

À l'inverse, l'Office a considéré qu'un traitement de données biométriques par le biais d'un dispositif de reconnaissance faciale ne pouvait être autorisé dans le but d'identifier des personnes au sein des stades de football[298]. En août 2019, l'Office se prononça sur un projet d'utilisation de la reconnaissance faciale afin d'identifier les supporters à l'entrée d'un stade. Il rappela que le traitement de données biométrique était strictement encadré par l'article 9 du RGPD et précisa que ni la loi tchèque sur la protection des données à

292 Úřad pro ochranu osobních údajů, « Kontrola používání technologie FaceID (společnost Metrostav a.s.) », 2019.

https://www.uoou.cz/kontrola-pouzivani-technologie-faceid-spolecnost-metrostav-a-s/ds-5677/archiv=0&p1=1277

293 Un projet est actuellement en réflexion afin d'intégrer la prise en compte des dispositifs biométriques au sein du Code du Travail. L'objectif étant de venir compléter l'actuel article 319 du code précité, relatif à la surveillance des employés (Mgr. Jan Ševčík Bc. Jiří Prouza, "Zpracování biometrických údajů zaměstnanců", 22 août 2019, https://www.epravo.cz/top/clanky/zpracovani-biometrickych-udaju-zamestnancu-109845.html#_ftn3

294 La mise en œuvre d'alternatives s'était en effet révélée inefficace.

295 Dès lors qu'il existe, en général d'autres moyens , moins intrusifs pour assurer la protection du chantier.

296 Úřad pro ochranu osobních údajů, *« k návrhu zákona, kterým se mění zákon č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů, a zákon č. 435/2004 Sb., o zaměstnanosti, ve znění pozdějších předpisů* », 29 juillet 2019, https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=35418

297 « *Oprávnění zaměstnavatele je v souladu se smyslem článku 9 a dalších obecného nařízení o ochraně osobních údajů koncipováno přiměřeně úzce. To mj. znamená, že se neumožňuje využívání biometrických údajů zaměstnanců k jiným účelům, včetně pouhé evidence docházky.* » Ibidem.

298 Úřad pro ochranu osobních údajů, « *ÚOOÚ k biometrické identifikaci nežádoucích osob na fotbalových stadionech* », 16 août 2019.
https://www.uoou.cz/uoou-k-nbsp-biometricke-identifikaci-nezadoucich-osob-na-fotbalovych-stadionech/d-35541

caractère personnel ni la loi tchèque sur la promotion du sport[299] ne permettait d'autoriser un traitement de données biométriques dans un tel cadre.

L'Office à la protection des données a considéré que l'utilisation de la reconnaissance faciale dans cette situation spécifique ne contrevenait pas au principe de proportionnalité et de minimisation des données.

299 La loi tchèque sur la promotion du sport concerne uniquement les mesures destinées à garantir l'ordre durant les manifestations sportives et ne peut suffire à fonder l'utilisation d'un dispositif de reconnaissance faciale généraliser à l'entrée des stades.

BIBLIOGRAPHIE

I. Législation

- Loi du 12 mars 2019 sur le traitement des données personnelles "Act No. 110/2019 Coll.", https://www.uoou.cz/en/assets/File.ashx?id_org=200156&id_dokumenty=1837

II. Prise de position des autorités régulatrices de la protection des données

- Úřad pro ochranu osobních údajů, « *ÚOOÚ k biometrické identifikaci nežádoucích osob na fotbalových stadionech* », 16 août 2019, https://www.uoou.cz/uoou-k-nbsp-biometricke-identifikaci-nezadoucich-osob-na-fotbalovych-stadionech/d-35541

- Úřad pro ochranu osobních údajů, « *Kontrola používání technologie FaceID (společnost Metrostav a.s.)* », 2019, https://www.uoou.cz/kontrola-pouzivani-technologie-faceid-spolecnost-metrostav-a-s/ds-5677/archiv=0&p1=1277

Royaume-Uni

I. Législation

S'il n'existe pas de cadre légal spécifique à la reconnaissance faciale au Royaume-Uni, le ***Data Protection Act* du 23 mai 2018 (A)**, le ***Human Act Rights* de 1998 (B)** et le ***Surveillance Camera Code of Practice de 2013 (C)*** posent les premières pierres à l'édifice d'un encadrement légal de cette technologie.

A - Le Data Protection Act du 23 mai 2018

La législation nationale relative aux traitements des données personnelles est le ***Data Protection Act* du 23 mai 2018**[300]. Elle transpose la directive Police-Justice et adapte la législation britannique au RGPD.

La reconnaissance faciale doit dès lors respecter les six principes de protection des données **(1)** et mettre en œuvre les garanties propres au traitement sensible **(2)**. Elle exige également pour le responsable de traitement de réaliser une analyse d'impact et de consulter préalablement l'*Information Commissionner's Office* **(3)**.

1. Les six principes de protection des données

L'utilisation de la reconnaissance faciale nécessite pour le responsable de traitement de se conformer aux six principes de protection des données personnelles établis par la **troisième partie du *Data Protection Act de 2018 :***

1. Le traitement des données à caractère personnel, à des fins d'applications de la loi, doit être licite et loyal. Aux termes des sections 35(4) et 35(5), le traitement peut reposer ou non sur le consentement. À défaut, trois exigences doivent être remplies :

    a. Le traitement doit être strictement nécessaire aux fins d'application de la loi.

    b. Le traitement doit également être nécessaire à l'exercice d'une fonction conférée à une personne par un texte législatif ou une règle de droit et il doit être nécessaire pour des raisons d'intérêt public majeur.

    c. Enfin, le responsable de traitement doit mettre en place un document approprié relatif au traitement sensible. La *High Court* de Cardiff s'est prononcée sur l'application de ce principe à des expérimentations menées par les forces de l'ordre au *MotorPoint Arena* et à *Queen's Street*. En s'appuyant sur l'obligation de *Common law* de prévenir et détecter les crimes, les juges ont affirmé que le traitement est nécessaire pour les intérêts légitimes de la police des Galles du Sud [301].

2. La finalité pour laquelle les données à caractère personnel sont collectées à toute occasion doit être spécifiée, explicite et légitime. Les données à caractère personnel ainsi collectées ne doivent pas être traitées d'une manière incompatible avec la finalité pour laquelle elles ont été collectées [302].

3. Les données à caractère personnel traitées à des fins d'applications de la loi doivent être adéquates, pertinentes et non excessives au regard de la finalité pour laquelle elles sont traitées[303].

4. Les données à caractère personnel traitées à des fins d'applications de la loi doivent être exactes et, le cas échéant, mises à jour. Toutes les mesures raisonnables doivent être prises pour garantir que les

300 Data Protection Act 2018, http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

301 High Court of Justice, Cardiff, *R (Bridges) v. CCSWP and SSHD*, [2019] EWHC 2341 (ADMIN), § 137, https://www.judiciary.uk/wp-content/uploads/2019/09/bridges-swp-judgment-Final03-09-19-1.pdf

302 Data Protection Act 2018, Section 36, *The second data protection principle*

303 Data Protection Act 2018, Section 37, *The third data protection principle*

données à caractère personnel qui sont inexactes, eu égard à la finalité répressive pour laquelle elles sont traitées, soient effacées ou rectifiées sans délai[304].

5. Les données personnelles traitées à des fins d'applications de la loi doivent être conservées pendant une durée n'excédant pas celle nécessaire à la réalisation de la finalité pour laquelle elles sont traitées [305].

1. Les données à caractère personnel doivent être traitées de manière à garantir une sécurité appropriée des données à caractère personnel, en utilisant des mesures techniques ou organisationnelles appropriées (et, dans ce principe, la « sécurité appropriée » comprend la protection contre le traitement non autorisé ou illégal et contre la perte, la destruction ou la détérioration accidentelle)[306].

L'usage de la reconnaissance faciale dans le cadre du maintien de l'ordre public ne saurait échapper à ces six principes directeurs établis par le *Data Protection Act* du 23 mai 2018. Pour être en conformité, les dispositifs doivent traiter au strict minimum les données personnelles des individus de façon licite, selon des finalités déterminées et de manière sécurisée. Ces données doivent également être exactes, et conservées dans un délai raisonnable.

2) Les garanties propres aux traitements sensibles

La Section 42 du *Data Protection Act 2018* établit des garanties propres aux traitements sensibles, lesquelles doivent nécessairement être prises en compte dans le cadre du déploiement de la reconnaissance faciale eu égard à la sensibilité des données biométriques. Le responsable du traitement doit ainsi disposer d'un document de politique générale approprié lorsqu'est mis en œuvre un traitement sensible fondé sur le consentement de la personne concernée ou une condition précisée à l'annexe 8[307]. Ce document explique les procédures visant à assurer le respect des principes de protection des données ainsi que les politiques de conservation et d'effacement des données à caractère personnel. Il doit être conservé, mis à jour et être à la disposition du Commissaire à l'Information en cas de demande.

Lorsque le traitement sensible est effectué par un sous-traitant pour le compte du responsable de traitement, le registre tenu par le sous-traitant doit comporter le fondement du traitement ainsi que la manière dont il satisfait aux exigences de licéité. Il doit également mentionner si les données à caractère personnel sont conservées et effacées conformément aux politiques de conservation et d'effacement des données. Si ces politiques n'ont pas été suivies, il doit en justifier les raisons.

3). L'obligation de réaliser une analyse d'impact et de consulter l'Information Commissioner's Office au préalable

La Section 64 du *Data Protection Act 2018* prévoit des dispositions relatives à l'étude d'impact – qui reprend les dispositions européennes en la matière (*cf.* Partie I.) – lorsqu'un type de traitement présente un risque élevé pour les droits et libertés des personnes.

La Section 65 du *Data Protection Act 2018* impose, en outre, au responsable du traitement de consulter l'*Information Commissionner's Office* avant que le traitement soit mis en œuvre si l'analyse d'impact [...] indique que le traitement entraînerait un risque élevé pour les droits et libertés des personnes (en l'absence de mesure visant à atténuer le risque)[308] .

---

304 Data Protection Act 2018, Section 38, *The fourth data protection principle*

305 *Ibidem.*, Section 39, *The fifth data protection principle*

306 *Ibidem.*, Section 40, *The sixth data protection principle*

307 Les conditions spécifiées à l'Annexe 8 sont l'intérêt public, l'administration de la justice, la protection des intérêts vitaux des individus, la protection des enfants et des personnes à risque, les données à caractère personnel déjà présentes dans le domaine public, la défense d'un droit en justice, les actes judiciaires, la prévention de la fraude et l'archivage

308 Data Protection Act 2018, Section 65 (2) : *"The controller must consult the Commissioner prior to the processing if a data protection impact assessment prepared under section 64 indicates that the processing of the data would result in a high risk to the rights and freedoms of individuals (in the absence of measures to mitigate the risk)" lll*

B - Le Human Rights Act 1998

La High Court de Cardiff s'est ainsi positionnée dans **le jugement *R. (Bridges) v. SWP & SSHD, 2019*** sur la conformité de l'utilisation de la reconnaissance faciale dans l'espace public par la police des Galles du Sud. Le juge a alors rappelé l'importance de rendre compatible le traitement des données biométriques avec le ***Human Rights Act 1998***[309] qui incorpore la Convention européenne des Droits de l'Homme dans le droit britannique. Il a conclu en ce sens que la reconnaissance faciale constitue une ingérence aux droits et libertés fondamentaux **(1)**, laquelle doit être justifiée **(2)** et poursuivre un but légitime et nécessaire dans une société démocratique **(3)**.

1) L'existence d'une ingérence

Dans **le jugement *R. (Bridges) v. SWP & SSHD, 2019***, la High Court de Cardiff a statué sur l'existence d'une ingérence au sens de l'**article 8 de la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales** lorsque sont utilisés des dispositifs de reconnaissance faciale en direct[310] .La juridiction galloise a jugé que le simple stockage de données biométriques est suffisant pour que le traitement tombe sous le coup de l'article 8[311]. Elle souligne notamment que l'utilisation de cette technologie implique nécessairement la capture, le stockage et le traitement des données biométriques d'un individu avant que ces dernières ne soient effacées[312]. Les juges ont dès lors écarté les arguments – tenants à la courte durée de conservation, à la présence de la personne dans l'espace public et le caractère manifeste au public des traits du visage d'une personne – invoqués pour écarter l'application des dispositions l'article 8[313].

2) L'existence d'une base légale

Dans **le jugement *R. (Bridges) v. SWP & SSHD, 2019***, les juges ont estimé qu'une législation spécifique n'était pas nécessaire en raison du caractère non intrusif de la reconnaissance faciale. Celle-ci ne nécessitant pas d'employer la force contrairement à la collecte d'empreintes, l'obligation générale de Common law de prévention et de détection des crimes et délits apporte une base légale suffisante pour justifier l'utilisation de la reconnaissance faciale[314].

En outre, la High Court a ajouté qu'une technologie nouvelle ne sort pas nécessairement du cadre de la réglementation existante et qu'il n'est pas toujours nécessaire de créer un cadre juridique sur cette mesure pour cette technologie[315]. Cette position contraste avec celle défendue par l'agence britannique de protection des données personnelles.

3) La poursuite d'un but légitime et nécessaire dans une société démocratique

Pour qu'une ingérence soit justifiée, elle doit satisfaire aux quatre critères dégagés par la Cour suprême dans l'**arrêt *Bank Mellat v. Her Majesty's Treasury (No 2) [2014] AC 700***[316]. L'objectif de la mesure poursuivie doit être suffisamment important pour justifier la restriction d'un droit fondamental. L'atteinte doit également être rationnellement liée à l'objectif. Ensuite, une mesure moins intrusive ne doit pas être réalisable sans compromettre de manière inacceptable l'objectif. Enfin, un juste équilibre doit être aménagé entre les droits de l'individu et les intérêts de la société[317] .

---

309 Human Rights Act 1998, http://www.legislation.gov.uk/ukpga/1998/42/contents

310 High Court of Justice, Cardiff, précédemment cité, §59

311 High Court of Justice, Cardiff, précédemment cité

312 High Court of Justice, Cardiff, précédemment cité

313 High Court of Justice, Cardiff, précédemment cité, §§ 53-57

314 High Court of Justice, Cardiff, précédemment cité, §§ 69-78

315 High Court of Justice, Cardiff, précédemment cité, §§ 84

316 Supreme Court, *Bank Mellat (Appellant) v Her Majesty's Treasury (Respondent)*, [2013] UKSC 38 & [2013] UKSC 39, https://www.supremecourt.uk/cases/docs/uksc-2011-0040-judgment.pdf

317 High Court of Justice, Cardiff, précédemment cité, §98

La juridiction galloise a considéré que l'utilisation de la reconnaissance faciale dans l'espace public à des fins policières ne soulevait pas de problème au regard des deux premiers critères, sans fournir toutefois de motivation détaillée[318]. Il apparaît cependant de façon évidente que l'utilisation d'un tel dispositif par les forces de l'ordre est motivée par la protection de l'ordre public conformément aux termes de l'**article 8 alinéa 2 de la Convention européenne des Droits de l'Homme.**

La motivation de la Cour sur la compatibilité du dispositif avec les deux derniers critères est en revanche plus détaillée, car ces derniers doivent être contrôlés strictement par la Cour[319]. Elle observe que la mesure prise ne constitue pas une ingérence disproportionnée et qu'un juste équilibre a été trouvé en s'appuyant sur plusieurs éléments de faits :

- Le déploiement était ouvert et transparent
- L'utilisation était limitée dans l'espace et le temps
- Le dispositif était déployé dans le but spécifique d'identifier des personnes particulières
- Personne n'a été arrêté à tort
- Personne ne s'est plaint du dispositif, à part le requérant pour des raisons de principe
- Les ingérences étaient limitées au traitement algorithmique quasiment instantané et à la suppression des données biométriques du requérant
- Aucun renseignement personnel n'a été mis à la disposition d'un agent humain
- Aucune donnée n'a été conservée
- Aucune tentative d'identification du requérant n'a eu lieu
- Aucun agent de police n'a parlé au requérant

C - Le Surveillance Camera Code of Practice de 2013

Le ***Surveillance Camera Code of Practice*** et les documents relatifs à la politique des forces de l'ordre sont également des bases juridiques pertinentes pour la mise en œuvre d'un dispositif de reconnaissance faciale sur l'espace public. En effet, dans sa décision **Cardiff, R (Bridges) v. CCSWP and SSHD**, la High Court[320] a reconnu ce code de bonnes pratiques de l'usage des caméras de surveillance comme une base juridique pertinente dans l'encadrement de l'utilisation de la reconnaissance faciale en direct (aussi appelée « automatique »).

Le Code s'applique uniquement à l'utilisation de systèmes de caméras de surveillance qui fonctionnent dans des lieux publics en Angleterre et au Pays de Galles, qu'il y ait ou non une visualisation en direct, ou un enregistrement d'images ou d'informations ou de données associées. Il ne s'applique en revanche pas à la surveillance dite « secrète » opérée par les autorités publiques (en matière de renseignement intérieur) ou par des personnes privées dans les lieux publics (par exemple, dans un centre commercial)[321].

L'objectif de ce Code est de garantir aux individus que les caméras de surveillance soient déployées pour les protéger, plutôt que pour les espionner. Le gouvernement considère que lorsqu'une surveillance manifeste dans des lieux publics poursuit un objectif légitime et répond à un besoin urgent, toute surveillance de ce type doit être qualifiée de « surveillance par consentement », et ce consentement de la part de la communauté doit être un consentement éclairé et non pas assumé par un opérateur de système. Toutefois, le **paragraphe 1.5 de ce Code** semble très alarmant :

> *« Dans le modèle britannique de maintien de l'ordre, les policiers sont considérés comme des citoyens en uniforme. Ils exercent leurs pouvoirs de police sur leurs concitoyens avec le consentement implicite*

318 High Court of Justice, Cardiff, précédemment cité, §99

319 High Court of Justice, Cardiff, précédemment cité, §§100-101

320 High Court of Justice, Cardiff, précédemment cité, §22 (2)

321 Surveillance Camera Code of Practice, Juin 2013, §§1.9-1.10, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/282774/SurveillanceCameraCodePractice.pdf

de ces derniers : on parle de « surveillance policière par consentement ». Ce concept implique que la légitimité du maintien de l'ordre aux yeux du public repose sur un consensus général de soutien qui découle de la transparence de leurs pouvoirs, de la démonstration de l'intégrité dans l'exercice de ces pouvoirs et de leur responsabilité à cet égard »[322].

Ce Code énonce donc les **12 principes directeurs** suivants qui s'appliquent à tout exploitant de **systèmes de caméras de surveillance dans les lieux publics**, lesquels sont donc applicables à l'utilisation de systèmes de reconnaissance faciale sur l'espace public[323] :

1. L'utilisation d'un système de caméras de surveillance doit toujours avoir un but précis, poursuivre un objectif légitime et être nécessaire pour répondre à un besoin urgent identifié[324].
2. Elle doit tenir compte de ses effets sur les personnes et sur leur vie privée, avec des examens réguliers[325] pour s'assurer que son utilisation reste justifiée.
3. Elle doit être aussi transparente que possible, avec notamment la publication d'une personne à contacter pour l'accès à l'information et les plaintes.
4. La responsabilité et l'obligation de rendre compte de toutes les activités liées aux systèmes de caméras de surveillance, y compris les images et les informations collectées, détenues et utilisées, doivent être clairement définies.
5. Des règles, des politiques et des procédures claires doivent être mises en place avant l'utilisation d'un système de caméras de surveillance, et elles doivent être communiquées à tous ceux qui doivent s'y conformer.
6. Les images et les informations ne doivent pas être stockées au-delà de ce qui est strictement nécessaire pour l'objectif déclaré d'un système de caméras de surveillance, et ces images et informations doivent être supprimées une fois que leur objectif a été atteint.
7. L'accès aux images et aux informations conservées doit être limité et des règles claires doivent être définies pour déterminer qui peut y avoir accès et dans quel but ; la divulgation des images et des informations ne doit avoir lieu que lorsqu'elle est nécessaire à cette fin ou à des fins répressives
8. Les opérateurs de systèmes de caméras de surveillance doivent tenir compte de toute norme opérationnelle[326], technique et de compétence approuvée concernant un système et sa finalité, et s'efforcer de respecter et de maintenir ces normes.
9. Les images et les informations des systèmes de caméras de surveillance doivent faire l'objet de mesures de sécurité appropriées afin de les protéger contre tout accès et utilisation non autorisés.

322 *Ibidem.*, §1.5, « *In the British model of policing, police officers are citizens in uniform. They exercise their powers to police their fellow citizens with the implicit consent of their fellow citizens. Policing by consent is the phrase used to describe this. It denotes that the legitimacy of policing in the eyes of the public is based upon a general consensus of support that follows from transparency about their powers, demonstrating integrity in exercising those powers and their accountability for doing so* », traduit par nous

323 *Ibidem.*, §2.6

324 *Ibidem.*, §3.1.1, « Ce but légitime et ce besoin pressant peuvent inclure : la sécurité nationale, la sûreté publique, le bien-être économique du pays, la prévention des troubles ou de la criminalité, la protection de la santé ou de la morale ou la protection des droits et des libertés d'autrui. », ("*Such a legitimate aim and pressing need might include national security, public safety, the economic well-being of the country, the prevention of disorder or crime, the protection of health or morals, or the protection of the rights and freedoms of others.*", traduit par nous)

325 *Ibidem.*, §3.2.3, « Toute utilisation de la reconnaissance faciale ou d'autres systèmes de reconnaissance de caractéristiques biométriques doit être clairement justifiée et proportionnée à l'objectif visé, et être validée de manière appropriée. Elle doit toujours impliquer une intervention humaine avant de prendre des décisions qui affectent négativement un individu. » ("*Any use of facial recognition or other biometric characteristic recognition systems needs to be clearly justified and proportionate in meeting the stated purpose, and be suitably validated4. It should always involve human intervention before decisions are taken that affect an individual adversely.*", traduit par nous)

326 *Ibidem.*, §4.8.1, « Les normes approuvées peuvent s'appliquer à la fonctionnalité du système, à l'installation ainsi qu'au fonctionnement et à la maintenance d'un système de caméras de surveillance. Ces normes sont généralement axées sur les installations de vidéosurveillance typiques, mais il peut y avoir des normes supplémentaires applicables lorsque le système possède des capacités avancées spécifiques telles que les systèmes (…) de reconnaissance faciale (…). » (*"Approved standards may apply to the system functionality, the installation and the operation and maintenance of a surveillance camera system. These are usually focused on typical CCTV installations, however there may be additional standards applicable where the system has specific advanced capability such as (…) facial recognition systems (…)."*, traduit par nous)

10. Des mécanismes d'examen et d'audit efficaces doivent être mis en place pour garantir le respect des exigences légales, des politiques et des normes dans la pratique, et des rapports réguliers doivent être publiés.
11. Lorsque l'utilisation d'un système de caméras de surveillance poursuit un objectif légitime et qu'il existe un besoin urgent de l'utiliser, il devrait alors être utilisé de la manière la plus efficace possible pour soutenir la sécurité publique et l'application de la loi dans le but de traiter les images et les informations ayant une valeur probante.
12. Toute information utilisée pour soutenir un système de caméras de surveillance, qui est comparée à une base de données de référence à des fins de comparaison, doit être exacte et tenue à jour[327].

Pour soutenir l'application pratique de ces principes directeurs, le Commissaire aux caméras de surveillance (*Surveillance Camera Commissioner*) est habilité à fournir des informations et des conseils sur les normes opérationnelles et techniques approuvées en la matière[328].

II. Position des autorités régulatrices de la protection des données

L'expérimentation de la reconnaissance faciale au Royaume-Uni a déclenché les prises de position de plusieurs autorités de contrôle ainsi que d'un comité parlementaire. L'***Information Commissionner's Office*** (A), le ***Surveillance Camera Commissionner*** (B) , le ***Biometrics Commissionner*** (C) et le ***Science and Technology Commitee*** (D) ont ainsi été amenés à se prononcer sur l'usage de cette technologie.

A - L'Information Commissioner's Office

L'*Information Commissioner's Office* (ICO) est l'autorité indépendante britannique créée pour défendre la protection des données personnelles des citoyens. Elle s'est prononcée, une première fois sur la reconnaissance faciale en rappelant l'obligation de réaliser une analyse d'impact relation à la protection des données personnelles préalablement à la mise en place d'un tel dispositif susceptible de présenter un risque élevé pour les droits et libertés des personnes. En effet, tout traitement de données biométriques dans le but d'identifier de manière unique une personne requiert ainsi une analyse d'impact.[329]

Par ailleurs, l'ICO s'est prononcé une deuxième fois sur la reconnaissance faciale, de manière indirecte, en publiant sa décision du 11 mars 2019 [330].En l'espèce, le plaignant avait demandé des informations à la police de Surrey concernant l'utilisation de la reconnaissance faciale et plus particulièrement à propos : de la réalisation préalable d'une analyse d'impact, des prestataires techniques impliqués, de la fréquence du recours au dispositif, des bases de données sollicitées, etc. En l'absence de réponse de la police, le plaignant a saisi le Commissaire à l'information qui a rappelé à la police ses obligations.

L'absence de réaction de la police de Surrey a amené l'ICO à publier sa décision, le 11 mars 2019. Elle y rappelle à la police l'obligation de respecter l'article 10 (1) du *Freedom of Information Act 2000* qui donne droit à tout administré de demander des renseignements auprès d'une autorité publique et d'obtenir une réponse. Si cette décision ne porte pas directement sur le dispositif de reconnaissance faciale en lui-même, elle souligne l'importance d'informer la population sur le recours policier à cette technologie ou, à tout le moins, de répondre à leur questionnement légitime en cas de sollicitation.

---

327 *Ibidem.*, §4.12.1, « Toute utilisation de technologies telles que les systèmes de reconnaissance faciale qui peuvent reposer sur l'exactitude d'informations générées ailleurs telles que des bases de données fournies par d'autres ne devrait pas être introduite sans une évaluation régulière pour s'assurer que les données sous-jacentes sont adaptées à l'objectif visé. » ("*Any use of technologies such as ANPR or facial recognition systems which may rely on the accuracy of information generated elsewhere such as databases provided by others should not be introduced without regular assessment to ensure the underlying data is fit for purpose*", traduit par nous)

328 *Ibidem.*, §1.7

329 Information Commissioner's Office, "Examples of processing 'likely to result in high risk' ", https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/examples-of-processing-likely-to-result-in-high-risk/

330 Information Commissioner's Office, Decision notice [FS50811107], 11 mars 2019, https://ico.org.uk/media/action-weve-taken/decision-notices/2019/2614559/fs50811107.pdf

Par la suite, dans **billet de blog publié le 25 juin 2019**[331] sur son site, l'ICO a alerté sur les risques de préjugés humains et de discriminations dans les systèmes d'intelligence artificielle. À ce titre, l'ICO prend pour exemple le risque de biais liés aux dispositifs de reconnaissance faciale en cas de déséquilibre dans les données d'entraînement (visages appartenant davantage à un genre particulier, une origine spécifique, etc.). Elle propose néanmoins des approches techniques pour atténuer le risque de discrimination et rappelle les obligations qui pèsent sur les organisations se dotant de dispositifs algorithmiques autoapprenants.

Dans un quatrième temps, l'*Information Commissioner*, Elizabeth Denham, a eu l'occasion de prendre une position affirmée sur l'usage de la reconnaissance faciale en direct au quartier de *King's Cross* à Londres par la voie d'une **déclaration en date du 15 avril 2019**[332]. Affirmant que la reconnaissance constituait un des sujets majeurs de l'ICO[333], elle a ouvert une enquête. Elle souligne également la nécessité d'examiner la suffisance du cadre légal en vigueur à l'époque face à ces technologies.

Au-delà des déclarations de l'ICO incitant les acteurs à faire preuve de coopération avec l'autorité indépendante, l'autorité a nuancé son apparente hostilité en lançant un **projet « *Sandbox* »** (bac à sable). Celui-ci a vocation à soutenir l'innovation technologique et l'utilisation des données en aménageant les exigences légales. Le 29 juillet 2019, l'ICO a sélectionné les dix premiers participants à ce projet[334] . Ils pourront s'appuyer sur l' expertise de l'autorité pour développer des dispositifs « *privacy by design* », atténuer les risques lors des expérimentations de ces innovations et assurer la mise en œuvre de garanties appropriées. Parmi les dix projets sélectionnés a été retenu celui de l'aéroport d'Heathrow Ltd qui prévoit l'automatisation de l'ensemble des contrôles des passagers de l'aéroport par l'utilisation de la biométrie – et notamment la reconnaissance faciale – de la phase d'enregistrement jusqu'à celle d'embarquement. Toutes les organisations participantes au projet *Sandbox* devraient le quitter d'ici septembre 2020 avec un rapport d'évaluation remis par l'ICO.

Dans un sixième temps, l'ICO s'est positionné plus précisément sur la question en soutenant une position en faveur de l'adoption d'un cadre normatif spécifique à la reconnaissance faciale. Dans une **opinion publiée le 31 octobre 2019**[335] **,** l'autorité britannique de protection des données a fait part de sa volonté de collaborer avec les autorités compétentes afin de renforcer le cadre juridique encadrant la reconnaissance faciale. Le régulateur souhaite que soit rédigé et publié un code de pratique dont la valeur serait contraignante. Celui-ci devrait s'appuyer sur les normes déjà établies par le Code sur les caméras de surveillance et mettre l'accent sur les spécificités de l'utilisation de la reconnaissance faciale par les forces de police.

Cette opinion témoigne des désaccords entre la High Court de Cardiff et l'autorité de contrôle. Dans le **jugement *R. (Bridges) v. SWP & SSHD, 2019***, les juges ont estimé qu'une législation spécifique n'était pas nécessaire en raison du caractère non intrusif de la reconnaissance faciale. Celle-ci ne nécessitant pas d'employer la force contrairement à la collecte d'empreintes, l'obligation générale de Common law de prévention et de détection des crimes et délits apporte, selon les juges, une base légale suffisante pour justifier l'utilisation de la reconnaissance faciale[336].

331 Information Commissioner's Office, "Human bias and discrimination in AI systems", 25 juin 2019, https://ico.org.uk/about-the-ico/news-and-events/ai-blog-human-bias-and-discrimination-in-ai-systems/

332 Information Commissioner's Opinion, "Statement: Live facial recognition technology in King's Cross",15 août 2019, https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/08/statement-live-facial-recognition-technology-in-kings-cross/

333 De vives préoccupations ont ainsi exprimées dans les médias, ce qui souligne, d'une part, l'absence de coopération et de communication entre les acteurs publics et privés britanniques, déployant des dispositifs de reconnaissance faciale, et l'ICO et, d'autre part, la place centrale que jouent tant la presse que les associations de défense des droits et libertés fondamentales en dénonçant de tels usages.

Pour les déclaration de l'ICO voy. *"Facial recognition technology is a priority area for the ICO and when necessary, we will not hesitate to use our investigative and enforcement powers to protect people's legal rights."*

334 Information Commissioner's Opinion, "ICO selects first participants for data protection Sandbox", 29 juillet 2019, https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-selects-first-participants-for-data-protection-sandbox/

335 Information Commissioner's Opinion, "The use of live facial recognition technology by law enforcement in public places", 31 octobre 2019, p. 3, https://ico.org.uk/media/about-the-ico/documents/2616185/live-frt-law-enforcement-report-20191031.pdf

336 High Court of Justice, Cardiff, précédemment cité, §§69-78

En tant qu'intervenant dans la procédure, l'autorité de contrôle a également soutenu que l'utilisation de la reconnaissance faciale par les forces de police et l'inscription d'individus sur une liste de surveillance devraient faire l'objet d'une autorisation indépendante de la part de la justice ou d'une autorité administrative[337]. La haute juridiction galloise n'a cependant pas partagé cette position. Elle considère en effet que la reconnaissance faciale en temps réel pas une forme d'outil secret de collecte de renseignements. Dès lors, une telle autorisation n'est pas nécessaire[338].

Face à ces divergences de position, le régulateur britannique estime que **le jugement *R. (Bridges) c. SWP & SSHD*** ne doit pas être interprété comme une autorisation générale d'utiliser la reconnaissance faciale en toutes circonstances en raison du principe de stricte nécessité du traitement consacré à l'**article 35§5(a) du *Data Protection Act 2018.*** Ainsi, l'utilisation de la reconnaissance faciale « pour localiser un terroriste ou un criminel violent dans une zone spécifique » est plus susceptible de remplir les exigences de proportionnalité qu'un « traitement généralisé, opportuniste et aveugle [...] de données biométriques appartenant à des milliers de personnes afin d'identifier quelques personnes d'intérêt mineur ou des personnes recherchées »[339].

Enfin, dans une **déclaration du 24 janvier 2020** en réponse à l'annonce faite par le service de police métropolitain de Londres (Met) sur l'utilisation de la reconnaissance faciale en direct, l'ICO a publiquement invité le Met à lui fournir de plus amples informations sur le projet.

Ce dernier a réitéré son appel au gouvernement pour qu'il introduise en priorité un code de pratique obligatoire et statutaire pour l'usage de la reconnaissance faciale en direct dans les lieux publics. Ce code garantirait l'uniformité de l'utilisation de cette technologie par les forces de police et améliorera la clarté et la prévisibilité de son utilisation pour le public et les policiers.

Par conséquent, la reconnaissance faciale demeure une priorité élevée pour l'ICO, qui aurait plusieurs enquêtes en cours. L'autorité prévoit, en outre, de publier prochainement sur l'utilisation par le secteur privé au cours de l'année 2020[340] .

B - Le Surveillance Camera Commissioner

Le ***Surveillance Camera Commissioner*** a été créé en vertu du ***Protection of Freedoms Act 2012*** qui réglemente la vidéosurveillance. Il a notamment pour rôle d'encourager le respect du Code de bonnes pratiques des caméras de surveillance (*Surveillance camera code of practice*) par les autorités compétentes. Il a un rôle de conseils sur l'utilisation efficace, appropriée, proportionnée et transparente des systèmes de caméras de surveillance et sur le respect des normes opérationnelles et techniques. Il n'a en revanche pas le pouvoir d'inspecter les opérateurs de vidéosurveillance pour vérifier qu'ils respectent ce Code.

Dans une **déclaration du 11 septembre 2019** rendue suite au jugement de la High Court sur l'utilisation de la technologie de reconnaissance faciale en direct par la police de Cardiff[341], le Commissaire aux caméras de surveillance a incité la police à faire preuve de prudence. Selon l'autorité, il ne faudrait pas considérer ce jugement d'espèce comme un feu vert pour le déploiement générique de la reconnaissance faciale en direct.

Il rappelle qu'il s'agit d'un outil intrusif ayant des implications sur les Droits de l'homme et la confiance du public qui doivent être prises en compte. Il existe cependant un sentiment accru de confiance que,

337 *Ibidem.*, §64

338 *Ibidem.*, §83

339 Information Commissioner's Opinion, précédemment cité, p. 21

340 Information Commissioner's Office, "ICO statement in response to an announcement made by the Metropolitan Police Service on the use of live facial recognition", 24 janvier 2020, https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/01/ico-statement-in-response-to-an-announcement-made-by-the-met-police/

341 Surveillance Camera Commissioner, "Statement on the High Court judgment on the use of Automatic Facial Recognition technology by South Wales police", 11 septembre 2019, https://www.gov.uk/government/publications/the-use-of-facial-recognition-technology-by-south-wales-police/statement-on-the-high-court-judgment-on-the-use-of-automatic-facial-recognition-technology-by-south-wales-police

dans des circonstances appropriées, une telle utilisation sera licite, mais doit être manifestement menée dans le cadre juridique et faire preuve de bonne gouvernance et de légitimité des efforts.

C - Biometrics Commissioner

Le ***Biometrics Commissioner*** (Commissaire à la biométrie) a été créé en vertu du ***Protection of Freedoms Act* de 2012**. Son rôle est de surveiller la conservation et l'utilisation par la police d'échantillons d'ADN, de profils d'ADN et d'empreintes digitales.

Le jugement de la High Court et l'annonce du Met sur l'utilisation de la technologie de reconnaissance faciale en direct ont suscité de nombreuses réactions des autorités régulatrices. Allant dans le même sens que l'*Information Commissioner's Office* et le *Surveillance Camera Commissioner*, le *Biometrics Commissioner* a précisé, dans une **annonce en date du 24 janvier 2020**[342], que si la cour a jugé l'utilisation de la reconnaissance faciale à Cardiff comme étant conforme aux exigences du *Human Rights Act* de 1998 et de la législation sur la protection des données, ce jugement était toutefois spécifique aux circonstances particulières dans lesquelles la police avait utilisé son système de reconnaissance faciale en direct. Le commissaire alerte donc la police métropolitaine de Londres, qui devra prêter attention aux circonstances sur lesquelles le tribunal a attiré l'attention.

Il souligne, par ailleurs, que cette décision fait actuellement l'objet d'un appel et que le nouveau gouvernement s'est engagé manifestement à fournir un cadre juridique strict pour régir l'utilisation future par la police de la biométrie et de l'intelligence artificielle.

Il appelle, enfin, à la conduite d'un débat citoyen afin d'examiner comment les technologies peuvent servir l'intérêt public tout en protégeant les droits des citoyens à une vie privée sans ingérence inutile de l'État ou des entreprises privées[343]

D - Science and Technology Committee

Dans un **rapport du 17 juillet 2019 sur le travail du Commissaire à la biométrie et du régulateur des sciences médico-légales**[344], le ***Science and Technology Committee*** (Comité des Sciences et de la Technologie de la Chambre des communes) insiste sur le fait que la reconnaissance faciale ne devrait pas être déployée tant que l'efficacité de la technologie et les risques de biais n'auront pas été élucidés. Il demande ainsi au Gouvernement de publier un moratoire sur l'utilisation actuelle de la technologie de reconnaissance faciale et d'interdire toute autre expérimentation tant qu'un cadre législatif n'aura pas été mis en place[345].

Selon le Comité, il importe que les images de personnes non condamnées ne soient pas conservées dans la base de données de la police. En effet, ces images pourraient constituer la base de « listes de surveillance » pour la technologie de reconnaissance automatique des visages lorsqu'elle est utilisée par les forces de police dans les espaces publics[346]. En 2015 déjà, le Comité biométrique avait critiqué l'absence d'un régime légal solide pour gouverner la détention des images de personnes innocentes aux fins de prévention de la criminalité. Cela faisait suite à une affaire portée devant la High Court en 2012 – ***R (RMC et FJ) contre MPS (Metropolitan Service de police)*** – dans laquelle la Haute Cour avait jugé que la détention indéfinie d'images de personnes innocentes les images des personnes détenues était illégale[347].

342 Biometrics Commissioner, "Response to announcement on Live Facial Recognition", 24 janvier 2020, https://www.gov.uk/government/news/response-to-announcement-on-live-facial-recognition

343 Biometrics Commissioner, "Biometrics Commissioner response to court judgment on South Wales Police's use of automated facial recognition technology", 10 septembre 2019, https://www.gov.uk/government/news/automated-facial-recognition

344 Science and Technology Committee, "The work of the Biometrics Commissioner and the Forensic Science Regulator", 17 juillet 2019, https://publications.parliament.uk/pa/cm201719/cmselect/cmsctech/1970/1970.pdf

345 *Ibidem.*, §37., p. 16

346 *Ibidem.*, §39, p. 17

347 High Court of Justice, London, *RMC and FJ v. Commissioner of Police for the Metropolis and Secretary of State for the Home Department* [2012] EWHC 1681 (Admin), §20, https://www.judiciary.uk/wp-content/uploads/JCO/Documents/Judgments/r-rmc-fj-metropolitan-police-commissioner-22062012.pdf

III. Cas d'usage

Le Royaume-Uni est l'un des États les plus avancés dans le déploiement de la reconnaissance faciale. Cette technologie y a été expérimentée à de multiples reprises dans des contextes et des environnements variés, plus spécifiquement sur la voie publique en dehors de tout évènement particulier **(A)**, lors d'évènements festifs **(B)**, dans les aéroports **(C)** et les gares **(D)**, les centres commerciaux **(E)** et dans des lieux d'exposition **(F)**. Nous développerons également un cas d'usage *sui generis* à King Cross **(G)**.

A - Les cas d'usage de la reconnaissance faciale sur la voie publique en dehors de tout évènement particulier

1. Londres

La police métropolitaine de Londres (Met) a mené plusieurs expérimentations de reconnaissance faciale en direct entre 2016 et 2019. L'une des expérimentations les plus médiatisées fut celle de Romford : en janvier 2019, la police a arrêté un individu qui se couvrait le visage puis a écopé d'une amende de 90 livres sterling. Selon le Met, l'individu a été interpellé par la police en raison d'agissements suspects. Il serait ensuite devenu agressif et aurait provoqué une altercation verbale avec les officiers, justifiant une amende [348]. Le *Financial Times* rapporte pourtant les propos d'un officier [349] expliquant que :

> « Le fait qu'il soit passé devant nous en masquant clairement son visage pour ne pas être reconnu nous donne des raisons de l'arrêter » [350]

Le maire de Londres assure toutefois que le refus de la reconnaissance faciale n'est pas un motif d'arrestation[351] . Il maintient que cette ligne de conduite est respectée par le Met [352] [353]. Cet épisode témoigne néanmoins du manque de légitimité que rencontre cette technologie auprès d'une partie de la population. L'ICO a observé qu'une analyse d'impact a été rédigée pour ce déploiement[354].

En janvier 2020, la police métropolitaine de Londres a annoncé qu'elle commencerait à recourir aux caméras de reconnaissance faciale en direct (« *live facial recognition* »), à compter du mois de février[355], dans des quartiers très fréquentés de la capitale. Il s'agit d'identifier les personnes recherchées pour délits graves, notamment la violence grave, les délits commis à l'aide d'armes à feu et à couteaux, l'exploitation sexuelle des enfants et à protéger les personnes vulnérables[356] . Une analyse d'impact a été publiée sur le site internet du Met [357].

---

348 L. Dearden, "Police stop people for covering their face from facial recognition camera then fine man £90 after he protested" [en ligne], *The Independent*, 31 janvier 2019, [consulté le 19/03/2020], https://www.independent.co.uk/news/uk/crime/facial-recognition-cameras-technology-london-trial-met-police-face-cover-man-fined-a8756936.html

349 M. Murgia, "How London became a test case for using facial recognition in democracies" [en ligne], *Financial Times*, 01 août 2019, [consulté le 17/01/2020], https://www.ft.com/content/f4779de6-b1e0-11e9-bec9-fdcab53d6959

350 M. Murgia, précédemment cité,*"The fact that he's walked past clearly masking his face from recognition. It gives us grounds to stop him"*, traduit par nous

351 The Mayor of London, "Live facial recognition technology trial in Romford (1)" [en ligne], *London Gov*, 22 mars 2019, [consulté le 19/03/2020], https://www.london.gov.uk/questions/2019/6099

352 The Mayor of London, "Live facial recognition technology trial in Romford (2)" [en ligne], *London Gov*, 19 mars 2019, [consulté le 19/03/2020], https://www.london.gov.uk/questions/2019/6100

353 The Mayor of London, "Live facial recognition technology trial in Romford (3)" [en ligne], *London Gov*, 17 mai 2019, [consulté le 19/03/2020], https://www.london.gov.uk/questions/2019/8888

354 Information Commissioner's Opinion, "The use of live facial recognition technology by law enforcement in public places", précédemment cité

355 V. Dodd, "Met police to begin using live facial recognition cameras in London" [en ligne], *The Guardian*, 24 janvier 2020, [consulté le 30/01/2020], https://www.theguardian.com/technology/2020/jan/24/met-police-begin-using-live-facial-recognition-cameras?CMP=fb_a-technology_b-gdntech

356 Metropolitan police, "Met begins operational use of Live Facial Recognition (LFR) technology" [en ligne], *Metropolitan police*, 24 janvier 2020, [consulté le 30/01/2020], http://news.met.police.uk/news/met-begins-operational-use-of-live-facial-recognition-lfr-technology-392451

357 Metropolitan police, « Data Protection Impact Assessment », [en ligne], *Metropolitan Police*, 10 février 2020, [consulté le 18/03/2020], https://www.met.police.uk/SysSiteAssets/media/downloads/central/advice/met/facial-recognition/data-protection-impact-assessment.pdf

Selon les déclarations du Met reportées dans *The Guardian*[358], les caméras sont liées à une base de données de suspects téléchargée à l'aide des derniers renseignements. En l'absence de concordance entre les visages détectés et la base de données, les données biométriques seront supprimées en quelques secondes. En cas de correspondance, une alerte sera générée auprès des agents supervisant le dispositif, qui décideront ou non de mobiliser un agent sur place. Le système ne sera pas lié à d'autres bases de données officielles.

Le Met a déclaré que le système était efficace à 70% pour repérer les suspects recherchés, mais ces résultats ont été contredits par le professeur Pete Fussey – un expert en surveillance de l'Université d'Essex – lors d'un examen indépendant. Ce dernier a en effet constaté que la précision était vérifiable dans seulement 19% des cas. Si le Met n'a pas réagi à cette enquête, il a reconnu auprès de *The Guardian* que son système était moins efficace pour balayer des foules denses[359]. Les derniers chiffres et résultats communiqués par la police londonienne semblent confirmer l'analyse du professeur : s'agissant du système de reconnaissance faciale en direct déployé sur l'avenue d'Oxford Circus, sur 8 600 visages scannés en une semaine, seules 8 personnes ont été identifiées de manière certaine[360], dont une seule personne était recherchée par la police[361] .Cela représente donc un taux de fausse identification de 87,5%.

2. Cardiff

La police des Galles du Sud a également expérimenté la reconnaissance faciale à Queen's Street, une zone commerçante achalandée de Cardiff, le 21 décembre 2017[362]. Une fourgonnette équipée de caméras dotées de la solution NeoFace était déployée dans la rue commerçante[363]. Ce projet pilote s'est déroulé en dehors de tout évènement particulier et a donné lieu à un recours intenté par Edward Bridges contre la police des Galles du Sud devant la High Court de Cardiff. Le jugement indique qu'une analyse d'impact a été réalisée par les forces de l'ordre [364] et est disponible sur le site internet de la police[365]. Notons toutefois que l'expérimentation litigieuse ne figure pas dans l'historique des déploiements.

B - Les cas d'usage de la reconnaissance faciale lors des évènements festifs

1. Londres

Les premières expérimentations, dans le cadre d'évènements festifs, ont eu lieu lors des 48e et 49e éditions du carnaval de Notting Hill en août 2016 et 2017. Le bilan de l'expérience fut néanmoins très mitigé : en août 2017, 98% des correspondances que le logiciel *NeoFace* – fourni par l'entreprise NEC – a reconnues comme positives ne l'étaient pas [366].

Ce programme informatique présente deux modes de fonctionnement :

- Le premier se nomme « *AFR Identify* » et permet l'identification de suspects inconnus et de personnes suspectées pour des crimes ou incidents passés. La base de données comprend environ 500 000 images.

---

358 V. Dodd, précédemment cité

359 *Ibidem.*

360 Y. Demeure, « Echec cuisant de la reconnaissance faciale à Londres » [en ligne], *Science post*, 12 mars 2020, [consulté le 12/03/2020], https://sciencepost.fr/londres-echec-cuisant-de-la-reconnaissance-faciale-a-londres/

361 B. Stephen, "London's Metropolitan Police scanned 8,600 people's faces without their consent last week" [en ligne], *The Verge*, 4 mars 2020, [consulté le 12/03/2020], https://www-theverge-com.cdn.ampproject.org/c/s/www.theverge.com/platform/amp/2020/3/4/21164482/london-metropolitan-police-face-scanning-consent-civil-liberties

362 High Court of Justice, Cardiff, précédemment cité, §11

363 High Court of Justice, Cardiff, précédemment cité, §11

364 High Court of Justice, Cardiff, précédemment cité, §§143-148

365 South Wales Police, « South Wales Police Data Protection Impact Assessment » [en ligne], South Wales Police, 11 octobre 2018, [consulté le 18/03/2020], http://afr.south-wales.police.uk/cms-assets/resources/uploads/DPIA-V5.4.pdf

366 V. Dodd, "UK police use of facial recognition technology a failure, says report" [en ligne], *The Guardian*, 15 mai 2018, [consulté le 30/01/2020], https://www.theguardian.com/uk-news/2018/may/15/uk-police-use-of-facial-recognition-technology-failure

- Le second mode « *AFR Locate* » extrait des images numériques du visage de membres du public à partir des flux de vidéosurveillance. Elles sont ensuite comparées aux données biométriques faciales des personnes qui figurent sur une liste de surveillance[367].

Une demande d'accès à l'analyse d'impact correspondant à la 48e édition du carnaval a été effectuée auprès de la police métropolitaine de Londres. Elle a été rejetée au motif que le document demandé serait destiné à une publication future[368]. Pourtant, nous ne sommes pas parvenus à nous la procurer. En revanche, une analyse d'impact en date du 25 juillet 2018 – se référant en introduction aux expérimentations menées au carnaval – est accessible sur le site de l'organisation à but non lucratif statewatch.org [369].

2. Cardiff

La police des Galles du Sud a également expérimenté la reconnaissance faciale à Cardiff pour la première fois le 3 juin 2017, lors de la finale de la Ligue des Champions[370]. Ce projet pilote a été réitéré ultérieurement à l'occasion d'un match du tournoi de rugby des Six Nations[371], des concerts de Kasabian et de Liam Gallagher[372], ou plus récemment au stade de Cardiff lors d'un match opposant Cardiff City à Swansea City[373]. L'objectif est de dissuader la réalisation d'actes malveillants et de prévenir les troubles à l'ordre public. Une analyse d'impact en date du 11 octobre 2018 a été effectuée par les forces de l'ordre et est accessible sur leur site internet[374]. En revanche, nous n'avons pas réussi à nous procurer de documents similaires à jour des évènements les plus récents.

L'utilisation de la reconnaissance faciale à l'occasion des évènements festifs fait l'objet de controverses. Des supporters et des militants des droits civiques ont ainsi manifesté devant le stade de Cardiff – avant le match du 12 janvier 2020 opposant Cardiff à Swansea – pour faire part de leur mécontentement et de leur inquiétude concernant l'usage de cette technologie[375].

L'expérimentation de cette technologie est également décriée pour son manque de fiabilité. Le projet pilote mené lors de la finale de la Ligue des Champions au *Principality Stadium* a rencontré un taux de correspondances erronées de 92%. Parmi les 170 000 spectateurs, 2 470 individus ont été identifiés comme des personnes d'intérêt dont 2 297 l'ont été à tort [376].

---

367 High Court, Cardiff, précédemment cité, §§ 26-29

368 Metropolitan police, « The use of Facial Recognition deployment at the Notting Hill Carnival 2017 » [en ligne], Metropolitan Police, [consulté le 18/03/2020] : https://www.met.police.uk/SysSiteAssets/foi-media/metropolitan-police/disclosure_2017/september_2017/information-rights-unit---the-use-of-facial-recognition-deployment-at-the-notting-hill-carnival-2017

369 Metropolitan police, « Metropolitan Police Service Privacy Impact Assessment » [en ligne], State Watch, [consulté le 18/03/2020], http://www.statewatch.org/news/2018/dec/uk-metropolitan-police-service-privacy-impact-assessment-lfr.pdf

370 South Wales Police, "Introduction of Facial Recognition into South Wales Police" [en ligne], South Wales Police, [consulté le 29/01/2020],https://www.south-wales.police.uk/en/news-room/introduction-of-facial-recognition-into-south-wales-police/

371 Information Commissionner's Office, "Investigation into how the police use facial recognition technology in public places", précédemment cité

372 South Wales Police, "Facial Recognition technology in partnership with South Wales Police" [en ligne], Motorpoint, 4 décembre 2017, [consulté le 29/01/2020], https://motorpointarenacardiff.co.uk/news-and-alerts/facial-recognition-technology-partnership-south-wales-police

373 T. Coleman, "South Wales Police to once again use facial recognition at Cardiff City v Swansea City derby match" [en ligne], *WalesOnline*, 8 janvier 2020, [consulté le 29/01/2020], https://www.walesonline.co.uk/sport/football/football-news/facial-recognition-cardiff-swansea-derby-17535425

374 South Wales Police, "South Wales Police Data Protection Impact Assessment" [en ligne], South Wales Police, 11 octobre 2018, [consulté le 18/03/2020], http://afr.south-wales.police.uk/cms-assets/resources/uploads/DPIA-V5.4.pdf

375 S. Morris, "Anger over use of facial recognition at South Wales football derby" [en ligne], *The Guardian*, 12 janvier 2020, [consulté le 29/01/2020], https://www.theguardian.com/technology/2020/jan/12/anger-over-use-facial-recognition-south-wales-football-derby-cardiff-swansea

376 Y. Demeure, « Pays de Galles : le taux de reconnaissance faciale de la police affiche un taux d'erreur affolant ! » [en ligne], Science Post, 9 mai 2018, [consulté le 12/03/2020], https://sciencepost.fr/pays-de-galles-la-reconnaissance-faciale-de-la-police-affiche-un-taux-derreur-affolant/

C - Les cas d'usage de la reconnaissance faciale dans les aéroports

1. Aéroport de Londres-Heathrow

Pour répondre aux exigences strictes de la *UK Border Force*, les aérogares 1 et 5 de l'aéroport d'Heathrow ont intégré, dès 2012, un système de reconnaissance faciale comme moyen d'authentification des passagers pour associer le visage d'un passager à sa carte d'embarquement[377].

De la même manière, la reconnaissance faciale est également utilisée comme moyen d'authentification par la *US Customs and Boarder Protection.* Le visage des passagers voyageant sur des vols à destination des États-Unis est scanné, enregistré et partagé avec le service de vérification des voyageurs. L'image enregistrée est ensuite comparée avec une galerie d'images des passagers du vol qui est alimentée à partir d'une base de données existante. La tentative de correspondance détermine si les passagers peuvent se rendre à ce point de contact, puis les images enregistrées sont immédiatement éliminées[378].

Cette solution est issue d'une collaboration entre Atkins (du groupe SNC-Lavalin) et l'entreprise britannique Aurora.

En 2017, dans un objectif d'améliorer l'efficacité et la fluidité de l'embarquement des passagers, mais aussi de réduire le personnel au sol, l'ensemble des compagnies membre de l'alliance Oneworld (British Airways, American Airlines, Iberia, etc.) ont déployé des portiques de reconnaissance faciale à l'aéroport londonien d'Heathrow. Ce projet qui marque une extension du recours à la reconnaissance faciale tant par les autorités de l'immigration que par les compagnies aériennes privées. L'authentification du passager se fait en deux temps : le visage du voyageur est d'abord scanné et enregistré lors de son passage au point de sécurité, puis il est scanné et comparé avec cet enregistrement lors de l'embarquement[379].

A la suite à plusieurs expérimentations, l'aéroport de Londres Heathrow a décidé de généraliser le recours à la reconnaissance faciale pour l'ensemble des étapes du transit des passagers[380].

Depuis l'été 2019 et jusqu'en avril 2020, l'aéroport Heathrow mène ainsi une expérimentation des systèmes de reconnaissance faciale sur la base du consentement des voyageurs. Les tests actuels ne sont liés à aucune base de données. Le dispositif utilise uniquement les données capturées pour évaluer les performances des équipements et des processus biométriques. Toutes les données recueillies auprès du passager sont conservées puis détruites dans les 30 jours et ne sont partagées avec aucun tiers[381].

Cette expérimentation s'inscrit dans le cadre du projet « *Sandbox* » supervisé par l'ICO (voir *supra*), il est donc possible de supposer qu'une analyse d'impact ait été réalisée conformément aux règles relatives à la protection des données personnelles.

2) Aéroport de Londres-Gatwick

Après une expérimentation d'auto-embarquement réalisée pendant une durée de trois mois en 2018 avec la compagnie Easyjet, l'aéroport de Gatwick est devenu, en 2019, le premier aéroport du Royaume-Uni à généraliser l'expérimentation de l'usage de la reconnaissance faciale comme moyen d'authentification des passagers. Cette expérimentation de six mois, qui s'est déroulée entre septembre 2019 et février 2020, a pour objectif de tester la technologie pour éventuellement la généraliser sur huit portes d'embarquement d'ici 2022[382].

---

377 SNC-Lavalin, « Système d'authentification des passagers par balayage » [en ligne], [consulté le 18/03/2020], https://www.snclavalin.com/fr-fr/projects/passenger-authentication-scanning-system

378 Heathrow, "Biometric testing", https://www.heathrow.com/at-the-airport/security-and-baggage/biometric-testing

379 S. Leblal, « La reconnaissance faciale se déploie aux portes d'embarquement à Heathrow » [en ligne], *Le monde informatique*, 10 avril 2017, [consulté le 17/03/2020], https://www.lemondeinformatique.fr/actualites/lire-la-reconnaissance-faciale-se-deploie-aux-portes-d-embarquement-a-heathrow-67889.html

380 En passant par les bornes d'enregistrement, les kiosques de dépose-bagage, aux contrôles de sécurité, jusqu'à l'embarquement

381 Heathrow, précédemment cité

382 L. Kelion, "Gatwick Airport commits to facial recognition tech at boarding" [en ligne], 17 septembre 2019, [consulté le 19/03/2020], https://www.bbc.com/news/technology-49728301

Cette expérimentation étant légalement fondée sur le consentement, le choix est laissé aux passagers de se faire contrôler leur passeport par du personnel humain. Toutefois, l'organisation non gouvernementale *Privacy International* a affirmé ses préoccupations quant au caractère éclairé du consentement au regard des simples panneaux généraux installés. L'ICO ne s'est toutefois pas prononcé sur ce cas d'espèce.

Par ailleurs, l'aéroport affirme qu'aucune donnée n'est stockée au-delà de la durée nécessaire pour les contrôles : les images sont supprimées quelques secondes après le dernier contrôle effectué.

D - Un cas d'usage de la reconnaissance faciale dans les gares

En 2017, des portiques *eGates*, développés par la société portugaise *Vision-Box*, ont été installés dans la gare internationale de Saint Pancras à Londres à des fins de contrôle aux frontières du Royaume-Uni. Ce portail vérifie l'identité des passagers par le biais d'un contrôle biométrique s'appuyant sur la technologie de reconnaissance faciale. L'image capturée par le dispositif est comparée à la photo stockée sur la puce du passeport. Ce projet a été réalisé en coopération avec Eurostar, la police des frontières françaises et le ministère français de l'Intérieur[383].

E - Les cas d'usage de la reconnaissance faciale dans les lieux d'exposition

1. Cardiff

La police du Sud du Pays de Galles a mis en place la reconnaissance faciale au Motorpoint Arena de Cardiff, un centre d'exposition couvert, lors du salon « Defence Procurement, Research, Technology and Exportability Exhibition » organisé en mars 2018. Les forces de l'ordre ont justifié l'utilisation du logiciel NeoFace en raison de la perturbation de l'évènement lors des éditions précédentes par quelques militants[384].Ces faits sont en outre à l'origine du recours introduit par Edward Bridges devant la High Court de Cardiff, déjà cité[385]. La décision de justice[386] se réfère à l'analyse d'impact effectuée par les forces de l'ordre également citées[387]. Pourtant, l'expérimentation litigieuse n'est pas mentionnée dans l'historique des déploiements.

2. Liverpool

Le *World Museum* de Liverpool a déployé un dispositif de reconnaissance faciale lors de l'exposition *« China's First Empereur and the Terracotta Warriors »* en 2018. Silkie Carlo, directeur de Big Brother Watch, alerte que ce dispositif aurait ciblé un nombre important d'écoliers [388]. Le *National Museums Liverpool* nuance ces mises en garde. Dans un courriel rédigé dans le cadre d'une demande d'accès à l'analyse d'impact [389], celui-ci indique :

> « Aucune évaluation de ce type n›a été réalisée car la technologie n›a pas été utilisée. Des caméras FRT ont été installées par mesure de précaution au cas où la menace terroriste s'intensifierait avant ou pendant l'exposition, auquel cas une escalade rapide des mesures de sécurité aurait été nécessaire. Aucune escalade ne s'étant produite, la technologie n'a pas été utilisée et aucune évaluation n'a donc été requise ». [390]

383 Passenger Self Service, "ABC EGates Installed At St. Pancras Rail Station" [en ligne], *Passenger Self Service*, 17 février 2017, [consulté le 19/03/2020], http://www.passengerselfservice.com/2017/02/abc-egates-installed-at-st-pancras-international-rail-station/

384 High Court of Justice, Cardiff, précédemment cité, §13

385 High Court of Justice, Cardiff, précédemment cité

386 High Court of Justice, Cardiff, précédemment cité §§143-148

387 South Wales Police, « South Wales Police Data Protection Impact Assessment » [en ligne], South Wales Police, 11 octobre 2018, [consulté le 18/03/2020], http://afr.south-wales.police.uk/cms-assets/resources/uploads/DPIA-V5.4.pdf

388 Big Brother Watch, "Facial Recognition 'Epidemic' in the UK" [en ligne], *Big Brother Watch*, 16 août 2019, [consulté le 17/01/2020], https://bigbrotherwatch.org.uk/all-media/facial-recognition-epidemic-in-the-uk/

389 What Does They Know, « FOI request 19/06 », [en ligne], National Museums Liverpool, 13 septembre 2019, [consulté le 18/03/2020], https://www.whatdotheyknow.com/request/597557/response/1431227/attach/3/FoI%20No.19%2006.pdf?cookie_passthrough=1

390 What Does They Know, précédemment cité,"No such assessment was completed as the technology was not used. FRT cameras were installed as a precautionary measure in case the threat of a terrorist was escalated before or during the exhibition,

Deux informations sont à retenir : d'une part, le dispositif aurait été seulement installé et n'aurait en conséquence pas été utilisé ; d'autre part, aucune analyse d'impact n'a été réalisée.

3. Birmingham

En août 2019, l'organisation non gouvernementale *Big Brother Watch* a dénoncé l'utilisation de la reconnaissance faciale à des fins de surveillance au *Millenium Point*, un centre de conférence de Birmingham. *Big Brother Watch* précise que des manifestations de syndicalistes, de supporters de footballs et de militants antiracistes ont déjà eu lieu aux alentours du centre de conférence [391]. En l'état de notre connaissance, nous ignorons si une analyse d'impact a été rédigée pour l'expérimentation menée.

F - Les cas d'usage de la reconnaissance faciale dans les centres commerciaux

1. Londres

La police métropolitaine de Londres a mené des expérimentations de reconnaissance faciale dans le centre commercial Westfield, situé dans le quartier de Stratford. Le logiciel utilisé est de nouveau « *NeoFace* » développé par la société NEC. Le taux de faux positif était alors de 81%[392]. Aucune analyse d'impact n'a été portée à notre connaissance.

2. Manchester

En octobre 2018, des officiers de la police du Grand Manchester étaient sous le feu des critiques pour avoir déployé la reconnaissance faciale pendant six mois pour surveiller les visiteurs du centre commercial *Trafford Centre*, le troisième plus grand complexe commercial du Royaume-Uni. Des points de contrôle ont été installés aux entrées du centre afin de reconnaître les personnes recherchées ou disparues. L'objectif était d'améliorer la sûreté et la sécurité du personnel et des éventuels clients. À ce titre, l'expérimentation menée a conduit à la réincarcération d'un individu.[393]

Le projet a néanmoins été critiqué avec virulence par le commissaire à la vidéosurveillance, Tony Porter. Celui-ci a témoigné de son inquiétude à l'égard de la disproportion du traitement et a souligné l'absence d'approbation de la haute hiérarchie policière sur cette expérimentation. Le déploiement a dès lors été arrêté [394]. En outre, nous ignorons l'existence d'une analyse d'impact en lien avec ce projet.

3. Sheffield

Une expérimentation de la reconnaissance faciale a également été menée dans le centre commercial *Meadowhall* de Sheffield en collaboration avec la police du Yorkshire du Sud. Celle-ci a duré quatre semaines entre janvier et mars 2018, à la fin de laquelle les données personnelles collectées ont été supprimées.

Elle a néanmoins souffert de lacunes en termes d'information et de communication. Aucun panneau avertissant les visiteurs sur le déploiement d'un tel dispositif n'avait été affiché. L'*Information Commissionner's Office* avait pourtant examiné l'expérimentation, mais a décidé de classer l'affaire sans prendre d'autres mesures[395]. De plus, aucune analyse d'impact n'a été portée à notre connaissance.

---

in which case a rapid escalation of security measures would have been required. As no such escalation occurred, the technology was not used and therefore no assessment was required", traduit par nous

391 Big Brother Watch, précédemment cité

392 P. Herard, « Reconnaissance faciale : nouvelles polémiques après l'échec cuisant de la police de Londres » [en ligne], TV5 Monde, 12 juillet 2019, [consulté le 17/01/2020], https://information.tv5monde.com/info/reconnaissance-faciale-nouvelles-polemiques-apres-l-echec-cuisant-de-la-police-de-londres

393 What Does They Know, "FREEDOM OF INFORMATION REQUEST REFERENCE NO: 002927/18", [en ligne], Great Manchester Police, 09 novembre 2018, [consulté le 18/03/2020], https://www.whatdotheyknow.com/request/527735/response/1262369/attach/html/2/0001%20RESPONSE%2020181109%20083715.DOC.doc.html

394 L. Randall, "Police used FACIAL recognition to monitor shopping centre visitors for SIX months" [en ligne], Daily Express, 15 octobre 2018, [consulté le 30/01/2020], https://www.express.co.uk/news/uk/1031939/manchester-news-police-surveillance-technology-trafford-centre-manchester

395 G. White and H. Clifton, "Meadowhall facial recognition scheme troubles watchdog" [en ligne], BBC News, 28 janvier 2020, [consulté le 30/01/2020], https://www.bbc.com/news/technology-51268093

G - Un cas d'usage de la reconnaissance faciale sui generis à King's Cross

Deux caméras dotées de la technologie de reconnaissance faciale ont été mises en place, entre mai 2016 et mars 2018, par la police de Camdem, sur le site de King's Cross qui est la propriété d'un consortium privé[396]. Les forces de l'ordre ont fourni des images de personnes recherchées, de suspects connus et de personnes disparues. L'objectif était d'aider *King's Cross Estate Services* à « s'acquitter de ses responsabilités en matière de prévention et de détection des crimes »[397]. Si le rapport de la police métropolitaine de Londres mentionne que le logiciel utilisé est développé par la société NEC[398], il ne fait aucun retour sur le succès de l'expérience. Un autre accord a été conclu le 5 janvier 2019 afin d'encadrer toute utilisation future de la reconnaissance faciale[399]. *King Cross Real Estate* affirme néanmoins ne plus utiliser cette technologie depuis mars 2018 [400]. Une demande d'accès à l'analyse d'impact a été réalisée auprès de *Transport For London*. N'étant pas à l'origine du projet, l'agence a affirmé ne détenir ni le document demandé ni avoir été consultée pour sa rédaction[401]. En tout état de cause, l'existence de cet audit échappe à notre connaissance.

396 D. Sabbagh, "Facial recognition technology scrapped at King's Cross site" [en ligne], *The Guardian*, 2 septembre 2019 [consulté le 31/01/20], https://www.theguardian.com/technology/2019/sep/02/facial-recognition-technology-scrapped-at-kings-cross-development

397 Metropolitan Police, "Report to the Mayor of London", 2019, §3, https://www.london.gov.uk/sites/default/files/040910_letter_to_unmesh_desai_am_report_re_kings_cross_data_sharing.pdf

398 *Ibidem.*, §6

399 *Ibidem.*, §13

400 King Cross, « Updated Statement : Facial Recognition » [en ligne], *King Cross Central Limited Partnership, 02 septembre 2019* [consulté le 18/03/2020], https://www.kingscross.co.uk/press/2019/09/02/facial-recognition

401 Transport For London, « FOI request detail Facial recognition King's Cross » [en ligne], *Transport For London,* 28 août 2019 [consulté le 18/03/2019], https://webcache.googleusercontent.com/search?q=cache:dut7Vzfko7oJ:https://tfl.gov.uk/corporate/transparency/freedom-of-information/foi-request-detail%3FreferenceId%3DFOI-1421-1920+&cd=6&hl=fr&ct=clnk&gl=fr

BIBLIOGRAPHIE

I. Législation

A - Lois

- Human Rights Act 1998, http://www.legislation.gov.uk/ukpga/1998/42/contents
- Data Protection Act 2018, http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted
- Surveillance Camera Code of Practice, Juin 2013, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/282774/SurveillanceCameraCodePractice.pdf

B - Jurisprudence

- High Court of Justice, Cardiff, *R (Bridges) v. CCSWP and SSHD*, [2019] EWHC 2341 (ADMIN), https://www.judiciary.uk/wp-content/uploads/2019/09/bridges-swp-judgment-Final03-09-19-1.pdf
- High Court of Justice, London, *RMC and FJ v. Commissioner of Police for the Metropolis and Secretary of State for the Home Department* [2012] EWHC 1681 (Admin), §20, https://www.judiciary.uk/wp-content/uploads/JCO/Documents/Judgments/r-rmc-fj-metropolitan-police-commissioner-22062012.pdf
- Supreme Court, *Bank Mellat (Appellant) v Her Majesty's Treasury (Respondent)*, [2013] UKSC 38 & [2013] UKSC 39, https://www.supremecourt.uk/cases/docs/uksc-2011-0040-judgment.pdf

II. Prise de position des autorités régulatrices de la protection des données

- Biometrics Commissioner, "Biometrics Commissioner response to court judgment on South Wales Police's use of automated facial recognition technology", 10 septembre 2019, https://www.gov.uk/government/news/automated-facial-recognition
- Biometrics Commissioner, "Response to announcement on Live Facial Recognition", 24 janvier 2020, https://www.gov.uk/government/news/response-to-announcement-on-live-facial-recognition
- Information Commissioner's Office, Decision notice [FS50811107], 11 mars 2019, https://ico.org.uk/media/action-weve-taken/decision-notices/2019/2614559/fs50811107.pdf
- Information Commissioner's Office, "Examples of processing 'likely to result in high risk' ", https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/examples-of-processing-likely-to-result-in-high-risk/
- Information Commissioner's Office, "Human bias and discrimination in AI systems", 25 juin 2019, https://ico.org.uk/about-the-ico/news-and-events/ai-blog-human-bias-and-discrimination-in-ai-systems/
- Information Commissioner's Opinion, "ICO selects first participants for data protection Sandbox", 29 juillet 2019, https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-selects-first-participants-for-data-protection-sandbox/
- Information Commissioner's Office, "ICO statement in response to an announcement made by the Metropolitan Police Service on the use of live facial recognition", 24 janvier 2020, https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/01/ico-statement-in-response-to-an-announcement-made-by-the-met-police/
- Information Commissioner's Opinion, "The use of live facial recognition technology by law enforcement in public places", 31 octobre 2019, https://ico.org.uk/media/about-the-ico/documents/2616185/live-frt-law-enforcement-report-20191031.pdf
- Information Commissioner's Opinion, "Statement: Live facial recognition technology in King's Cross",15 août

2019, https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/08/statement-live-facial-recognition-technology-in-kings-cross/

- Science and Technology Committee, "The work of the Biometrics Commissioner and the Forensic Science Regulator", 17 juillet 2019, https://publications.parliament.uk/pa/cm201719/cmselect/cmsctech/1970/1970.pdf
- Surveillance Camera Commissioner, "Statement on the High Court judgment on the use of Automatic Facial Recognition technology by South Wales police", 11 septembre 2019, https://www.gov.uk/government/publications/the-use-of-facial-recognition-technology-by-south-wales-police/statement-on-the-high-court-judgment-on-the-use-of-automatic-facial-recognition-technology-by-south-wales-police

III. Presse numérique

- Big Brother Watch, "Facial Recognition 'Epidemic' in the UK" [en ligne], *Big Brother Watch*, 16 août 2019, [consulté le 17/01/2020], https://bigbrotherwatch.org.uk/all-media/facial-recognition-epidemic-in-the-uk/
- Coleman T., "South Wales Police to once again use facial recognition at Cardiff City v Swansea City derby match" [en ligne], *WalesOnline*, 8 janvier 2020, [consulté le 29/01/2020], https://www.walesonline.co.uk/sport/football/football-news/facial-recognition-cardiff-swansea-derby-17535425
- Dearden L., "Police stop people for covering their face from facial recognition camera then fine man £90 after he protested" [en ligne], *The Independent*, 31 janvier 2019, [consulté le 19/03/2020], https://www.independent.co.uk/news/uk/crime/facial-recognition-cameras-technology-london-trial-met-police-face-cover-man-fined-a8756936.html

- Demeure Y., « Pays de Galles : le taux de reconnaissance faciale de la police affiche un taux d'erreur affolant ! » [en ligne], *Science Post*, 9 mai 2018 [consulté le 12/03/2020], https://sciencepost.fr/pays-de-galles-la-reconnaissance-faciale-de-la-police-affiche-un-taux-derreur-affolant/
- Demeure Y., « Echec cuisant de la reconnaissance faciale à Londres » [en ligne], *Science Post*, 12 mars 2020, [consulté le 12/03/2020], https://sciencepost.fr/londres-echec-cuisant-de-la-reconnaissance-faciale-a-londres/
- Dodd V., "Met police to begin using live facial recognition cameras in London" [en ligne], *The Guardian*, 24 janvier 2020, [consulté le 30/01/2020], https://www.theguardian.com/technology/2020/jan/24/met-police-begin-using-live-facial-recognition-cameras?CMP=fb_a-technology_b-gdntech
- Dodd V., "UK police use of facial recognition technology a failure, says report" [en ligne], *The Guardian*, 15 mai 2018, [consulté le 30/01/2020], https://www.theguardian.com/uk-news/2018/may/15/uk-police-use-of-facial-recognition-technology-failure
- Heathrow, "Biometric testing" [en ligne], [consulté le 18/03/2020], https://www.heathrow.com/at-the-airport/security-and-baggage/biometric-testing
- Herard P., « Reconnaissance faciale : nouvelles polémiques après l'échec cuisant de la police de Londres » [en ligne], *TV5 Monde*, 12 juillet 2019, [consulté le 17/01/2020], https://information.tv5monde.com/info/reconnaissance-faciale-nouvelles-polemiques-apres-l-echec-cuisant-de-la-police-de-londres
- Kelion L., "Gatwick Airport commits to facial recognition tech at boarding" [en ligne], 17 septembre 2019, [consulté le 19/03/2020], https://www.bbc.com/news/technology-49728301
- King Cross, « Updated Statement : Facial Recognition » [en ligne], *King Cross Central Limited Partnership*,

02 septembre 2019 [consulté le 18/03/2020], https://www.kingscross.co.uk/press/2019/09/02/facial-recognition

❖ Leblal S., « La reconnaissance faciale se déploie aux portes d'embarquement à Heathrow » [en ligne], *Le monde informatique*, 10 avril 2017, [consulté le 17/03/2020], https://www.lemondeinformatique.fr/actualites/lire-la-reconnaissance-faciale-se-deploie-aux-portes-d-embarquement-a-heathrow-67889.html

❖ Metropolitan police, « Data Protection Impact Assessment », [en ligne], *Metropolitan Police*, 10 février 2020, [consulté le 18/03/2020], https://www.met.police.uk/SysSiteAssets/media/downloads/central/advice/met/facial-recognition/data-protection-impact-assessment.pdf

❖ Metropolitan police, "Met begins operational use of Live Facial Recognition (LFR) technology" [en ligne], *Metropolitan police*, 24 janvier 2020, [consulté le 30/01/2020], http://news.met.police.uk/news/met-begins-operational-use-of-live-facial-recognition-lfr-technology-392451

❖ Metropolitan Police, "Report to the Mayor of London" [en ligne], 2019, [consulté le 31/01/2020], https://www.london.gov.uk/sites/default/files/040910_letter_to_unmesh_desai_am_report_re_kings_cross_data_sharing.pdf

❖ Metropolitan police, « Metropolitan Police Service Privacy Impact Assessment » [en ligne], *State Watch*, 25 juillet 2018 [consulté le 18/03/2020], http://www.statewatch.org/news/2018/dec/uk-metropolitan-police-service-privacy-impact-assessment-lfr.pdf

❖ Metropolitan police, « The use of Facial Recognition deployment at the Notting Hill Carnival 2017 » [en ligne], *Metropolitan Police,* [consulté le 18/03/2020] : https://www.met.police.uk/SysSiteAssets/foi-media/metropolitan-police/disclosure_2017/september_2017/information-rights-unit---the-use-of-facial-recognition-deployment-at-the-notting-hill-carnival-2017

❖ Morris S., "Anger over use of facial recognition at South Wales football derby" [en ligne], *The Guardian*, 12 janvier 2020, [consulté le 29/01/2020], https://www.theguardian.com/technology/2020/jan/12/anger-over-use-facial-recognition-south-wales-football-derby-cardiff-swansea

❖ Murgia M., "How London became a test case for using facial recognition in democracies" [en ligne], Financial Times, 01 août 2019, [consulté le 17/01/2020], https://www.ft.com/content/f4779de6-b1e0-11e9-bec9-fdcab53d6959

❖ Murgia M., « London's King's Cross uses facial recognition in security cameras » [en ligne], *Financial Times*, 12 août 2019, [consulté le 17/01/2020], https://www.ft.com/content/8cbcb3ae-babd-11e9-8a88-aa6628ac896c

❖ Passenger Self Service, "ABC EGates Installed At St. Pancras Rail Station" [en ligne], *Passenger Self Service*, 17 février 2017, [consulté le 19/03/2020], http://www.passengerselfservice.com/2017/02/abc-egates-installed-at-st-pancras-international-rail-station/

❖ Randall L., "Police used FACIAL recognition to monitor shopping centre visitors for SIX months" [en ligne], *Daily Express*, 15 octobre 2018, [consulté le 30/01/2020], https://www.express.co.uk/news/uk/1031939/manchester-news-police-surveillance-technology-trafford-centre-manchester

❖ Sabbagh D., "Facial recognition technology scrapped at King's Cross site" [en ligne], *The Guardian*, 2 septembre 2019 [consulté le 31/01/20], https://www.theguardian.com/technology/2019/sep/02/facial-recognition-technology-scrapped-at-kings-cross-development

- SNC-Lavalin, « Système d'authentification des passagers par balayage » [en ligne], [consulté le 18/03/2020], https://www.snclavalin.com/fr-fr/projects/passenger-authentication-scanning-system
- South Wales Police, « South Wales Police Data Protection Impact Assessment » [en ligne], South Wales Police, 11 octobre 2018, [consulté le 18/03/2020], http://afr.south-wales.police.uk/cms-assets/resources/uploads/DPIA-V5.4.pdf
- South Wales Police, "Facial Recognition technology in partnership with South Wales Police" [en ligne], *Motorpoint*, 4 décembre 2017, [consulté le 29/01/2020], https://motorpointarenacardiff.co.uk/news-and-alerts/facial-recognition-technology-partnership-south-wales-police
- South Wales Police, "Introduction of Facial Recognition into South Wales Police" [en ligne], *South Wales Police*, [consulté le 29/01/2020], https://www.south-wales.police.uk/en/news-room/introduction-of-facial-recognition-into-south-wales-police/
- Stephen B., "London's Metropolitan Police scanned 8,600 people's faces without their consent last week" [en ligne] , The Verge, 4 mars 2020, [consulté le 12/03/2020], https://www-theverge-com.cdn.ampproject.org/c/s/www.theverge.com/platform/amp/2020/3/4/21164482/london-metropolitan-police-face-scanning-consent-civil-liberties
- The Mayor of London, "Live facial recognition technology trial in Romford (1)" [en ligne], *London Gov*, 22 mars 2019, [consulté le 19/03/2020], https://www.london.gov.uk/questions/2019/6099
- The Mayor of London, "Live facial recognition technology trial in Romford (2)" [en ligne], *London Gov*, 19 mars 2019, [consulté le 19/03/2020], https://www.london.gov.uk/questions/2019/6100
- The Mayor of London, "Live facial recognition technology trial in Romford (3)" [en ligne], *London Gov*, 17 mai 2019, [consulté le 19/03/2020] , https://www.london.gov.uk/questions/2019/8888
- Transport For London, « FOI request detail Facial recognition King's Cross » [en ligne], *Transport For London,* 28 août 2019 [consulté le 18/03/2019], https://webcache.googleusercontent.com/search?q=cache:dut7Vzfko7oJ:https://tfl.gov.uk/corporate/transparency/freedom-of-information/foi-request-detail%3FreferenceId%3DFOI-1421-1920+&cd=6&hl=fr&ct=clnk&gl=fr
- What Does They Know, « FREEDOM OF INFORMATION REQUEST REFERENCE NO: 002927/18 », [en ligne], *Great Manchester Police*, 09 novembre 2018, [consulté le 18/03/2020], https://www.whatdotheyknow.com/request/527735/response/1262369/attach/html/2/0001%20RESPONSE%2020181109%20083715.DOC.doc.html
- What Does They Know, « FOI request 19/06 », [en ligne], *National Museums Liverpool*, 13 septembre 2019, [consulté le 18/03/2020], https://www.whatdotheyknow.com/request/597557/response/1431227/attach/3/FoI%20No.19%2006.pdf?cookie_passthrough=1
- White G. and Clifton H., "Meadowhall facial recognition scheme troubles watchdog" [en ligne], *BBC News*, 28 janvier 2020, [consulté le 30/01/2020], https://www.bbc.com/news/technology-51268093

Suède

I. Le cadre législatif suédois

Il n'existe pas de législation spécifique à la reconnaissance faciale en Suède. L'Autorité suédoise de protection des données, la *Datainspektionen,* a toutefois appelé le gouvernement à se saisir du sujet à l'occasion d'une consultation préalable sur les activités pilotes prévues par la police concernant la vérification biométrique du visage aux frontières extérieures.

L'encadrement des traitements de données à caractère personnel est assuré par la **loi (2018:218)**[402]. La législation suédoise comprend également un corpus de règles spécifiques dans la **loi (2018:1693)**[403] **sur le traitement des données à caractère personnel par la police dans le cadre de la loi sur les données criminelles**. Cette loi s'applique en sus des dispositions de **la loi (2018:1177)**[404] **sur les données criminelles**.

II. Position de l'autorité de contrôle

L'autorité de contrôle n'a pas formulé d'avis général sur la question. Elle a toutefois pris position dans divers cas particuliers étudiés à la section suivante. Nous retenons que la *Datainspektionen,* bien que prudente, est relativement favorable au recours à la technologie.

III. Cas d'usages

Trois cas d'usage seront ici présentés :

- ⇨ Dans le cadre de l'utilisation par les autorités de police suédoise d'un logiciel de reconnaissance faciale dans le cadre des **enquêtes policières** (A);
- ⇨ Pour l'utilisation de la reconnaissance faciale en matière de contrôle d'accès à **l'aéroport de Skavsta** (B);
- ⇨ Sur l'usage de la reconnaissance faciale au sein du **lycée Skellefteå (C)**. Ce dernier cas d'études a donné lieu à la première sanction prononcée par une autorité de protection des données en Europe au sujet de la reconnaissance faciale[405].

Nous étudierons donc successivement ces différentes prises de position du régulateur suédois.

A - Usages de la reconnaissance faciale par les forces de police

En 2019, la police suédoise réalisa une première expérimentation visant à comparer les images obtenues par le biais des caméras de vidéosurveillance en circuit fermé avec les données contenues dans des bases de données biométriques de criminels[406]. Une base de données réunissant 40 000 images de personnes répertoriées à la suite d'un crime ou d'une suspicion d'infraction a été créée à cette occasion. En dépit de résultats mitigés[407], la police souhaitait pérenniser le dispositif.

---

402 Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning, https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2018218-med-kompletterande-bestammelser_sfs-2018-218

403 Lag (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-20181693-om-polisens-behandling-av_sfs-2018-1693

404 Brottsdatalag (2018:1177) https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/brottsdatalag-20181177_sfs-2018-1177

405 Voy. *infra.*

406 C. Burt, « Police facial recognition off in Orlando, on in Netherlands and considered in Sweden » [en ligne], *BiometricUpdate*, 22, juillet 2019, [consulté le 30/01/2020], https://www.biometricupdate.com/201907/police-facial-recognition-off-in-orlando-on-in-netherlands-and-considered-in-sweden

407 Lors du test 83 images ont été soumises au dispositif avec un taux de correspondances avoisinant les 25%.

Dans un avis en date du 23 octobre 2019[408], l'autorité suédoise de protection des données se prononça sur l'utilisation d'un logiciel de reconnaissance faciale par les forces de police. Elle a autorisé celles-ci à utiliser la technologie, considérant qu'elles justifiaient d'un intérêt légitime « à traiter les données à caractère personnel de la manière proposée »[409]. Conformément à **l'article 1 du Chapitre 2 de la loi (2018:1177) sur les données relatives à la criminalité**, les forces de police ont la possibilité de traiter des données à caractère personnel dans le cadre de la prévention et de la détection des activités criminelles, en vue d'enquêter sur les infractions pénales et de les sanctionner. Selon l'autorité de protection, les finalités visées par le déploiement de dispositifs de reconnaissance faciale aux fins d'analyses judiciaires, d'enquêtes et de comparaisons ne contrevenaient pas aux principes édictés par **l'article 1 paragraphe 2 du Chapitre 6 de la loi (2018:1693) relative aux données pénales**.

Concernant le traitement des données sensibles, les forces de police[410] ont la possibilité de rechercher des données à caractère personnel telles que les données de santé, biométriques ou génétiques comprises dans les registres susmentionnés (**Chap.6 art.5 de la loi 2018 : 1693**). Celles-ci comprennent notamment les données traitées dans les registres de profils ADN, d'empreintes digitales et de signalisation.

L'autorité de protection des données considère que le traitement de données biométriques par la police est également admis dès lors qu'ils sont « absolument nécessaires aux fins du traitement »[411] conformément à l'**article 4 du Chapitre 6 de la loi (2018 : 1693**). Afin de justifier le caractère d'absolue nécessité, l'autorité de contrôle se fonde sur un arrêt de la Cour de justice des Communautés européennes(C-524/06) [412]. Faisant application de cette analyse jurisprudentielle la *Datainspektionen* a pu considérer que l'utilisation de la reconnaissance faciale dans le cadre des missions de police pouvait s'avérer « beaucoup plus efficace »[413] que le visionnage des images de vidéo surveillance par des agents.

B - Usages de la reconnaissance faciale au sein de l'aéroport de Skavsta

En décembre 2019, la police suédoise a consulté l'autorité de protection des données dans la perspective de mettre en œuvre un dispositif de reconnaissance faciale pour la surveillance des frontières au sein de l'aéroport de Skavsta[414]. Le logiciel VeriScan, développé par le *Metropolitan Washington Airports Authority,* devait à être utilisé.

Le projet se divisait en deux phases distinctes.

- ⇨ Dans un premier temps, les autorités devaient placer des caméras aux postes de contrôle frontalier afin de permettre de comparer une photo prise à celle présente dans le passeport. Cette première phase était nécessaire à la constitution d'une base d'images faciales.
- ⇨ Dans un second temps, cette collecte devait permettre le développement d'un algorithme permettant aux autorités d'utiliser le logiciel comme « aide à la décision pour le contrôle du document de voyage présenté »[415], en limitant le risque de discriminations.

La *Datainspektionen* fut consultée par la police suédoise en décembre 2019, qui avait au préalable transmis

---

408 Datainspektionen, « Polisen får använda ansiktsigenkänning för att utreda brott », 24 octobre 2019, https://www.datainspektionen.se/nyheter/polisen-far-anvanda-ansiktsigenkanning-for-att-utreda-brott/

409 Avis du 23 octobre 2019 de la Datainspektionen, « *Datainspektionen anser att Polismyndigheten har ett berättigat intresse av att behandla personuppgifter på det sätt man föreslagit.* », Traduit par nous.

410 En dépit des interdictions formulées à l'**article 14 du chapitre 2 de la loi sur les données criminelles.**

411 Avis du 23 octobre 2019 de la Datainspektionen, « *[…] får behandlas om det är absolut nödvändigt för ändamålet med behandlingen* », Traduit par nous

412 CJCE, n° C-524/06, Arrêt de la Cour, Heinz Huber contre Bundesrepublik Deutschland, 16 décembre 2008

413 Avis du 23 octobre 2019 de la Datainspektionen, « *[…] med ansiktsigenkänningsteknik för att identifiera gärningspersoner är betydligt effektivare än att enskilda tjänstemän gör denna selektering manuellt* », Traduit par nous

414 L. Pascu, « VeriScan biometrics surpass 1M air passengers processed as Japan, Jamaica, Sweden add checks » [en ligne] , *BiometricUpdate.com*, december 17, 2019, [consulté le 30/01/2020], https://www.biometricupdate.com/201912/veriscan-biometrics-surpass-1m-air-passengers-processed-as-japan-jamaica-sweden-add-checks

415 Avis de la datainspektionen du 16 décembre 2019, « Under fas två kommer uppgifterna hanteras avgränskontrollanter vid Skavsta flygplats som ett beslutsstöd för kontroll motden resehandling som uppvisas », Traduit par nous

une analyse d'impact.

L'autorité de contrôle considéra que la seconde phase, seule, était conforme au droit de la protection des données[416], le traitement prévu s'inscrivant dans les exceptions de l'article 9 du RGPD. La première phase ne l'était pas. Selon l'autorité, le cadre juridique permettant le traitement des données sensibles faisait en l'espèce défaut.

C - Usages de la reconnaissance faciale au sein lycée de Skellefteå

En 2018, un lycée de la ville de Skellefteå a expérimenté pendant une durée de trois semaines un logiciel de reconnaissance faciale. L'objectif poursuivi était de compléter le système classique d'appel réalisé par les agents de l'établissement, par un traitement de données biométriques et l'utilisation d'un logiciel de reconnaissance faciale[417]. Le projet expérimental impliquait 22 étudiants.

L le 20 août 2019, l'autorité de protection des données personnelles suédoise condamna le lycée au paiement d'une amende de 200 000 SEK[418]. Le dispositif adopté méconnaissait pour le RGPD[419] . La *Datainspektionen* releva :

- Premièrement, qu'elle n'avait pas été consultée en amont de l'expérimentation[420].

- Deuxièmement, que le consentement ne pouvait pas constituer une base légale pour le traitement des données personnelles dans le cadre de cette expérimentation[421] ; il n'était pas valide en l'espèce : « [d]ans le domaine scolaire, il est clair que l'élève est dans une position de dépendance vis-à-vis de l'école en termes de notes, de financement des études, d'éducation et donc de possibilité de travail futur ou de poursuite d'études. »[422].

Notons que les juridictions françaises de première instance suivront le même raisonnement concernant les lycées de la Région Sud.[423]

- Troisièmement, que les deux autres exceptions prévues à l'article 6 du RGPD ne pouvaient davantage être mobilisées. En effet, la loi sur les écoles (2010 : 800)[424] dispose qu'en cas d'absence sans motif valable d'un élève, le directeur d'école est dans l'obligation d'informer le responsable légal de l'élève de cette absence le jour même, conformément au §16 du chapitre 15 de cette même loi. Le régulateur suédois considéra que le traitement des données à caractère personnel devait être strictement nécessaire pour réaliser cette obligation, mais affirma qu'aucune des dispositions du droit national ne permettait de fonder le traitement des données sensibles. Ainsi, même s'il est possible « d'établir

416 Datainspektionen, « Lagändring krävs för att polisen ska kunna utföra testverksamhet av ansiktsverifiering på flygplats », 16 décembre 2019, https://www.datainspektionen.se/nyheter/lagandring-kravs-for-att-polisen-ska-kunna-utfora-testverksamhet-av-ansiktsverifiering-pa-flygplats/

417 E. Lefaix, « RGPD : Première amende pour la Suède après avoir utilisé la reconnaissance faciale dans un lycée » [en ligne], *SiècleDigital*, 28 août 2019, [consulté le 01/02/2020], https://siecledigital.fr/2019/08/28/amende-suede-reconnaissance-faciale-rgpd/

418 Soit l'équivalent de 19000 euros

419 E. Lefaix, « RGPD : Première amende pour la Suède après avoir utilisé la reconnaissance faciale dans un lycée » [en ligne], *SiècleDigital*, 28 août 2019, [consulté le 01/02/2020], https://siecledigital.fr/2019/08/28/amende-suede-reconnaissance-faciale-rgpd/

420 Datainspektionen, « *Tillsyn enligt EU:s dataskyddsförordning 2016/679 – ansiktsigenkänning för närvarokontroll av elever* », 20 août 2019, https://www.datainspektionen.se/globalassets/dokument/beslut/beslut-ansiktsigenkanning-for-narvarokontroll-av-elever-dnr-di-2019-2221.pdf

421 Pour rappel, le considérant n°43 du RGPD dispose que : « *le consentement n'est pas un fondement juridique valable pour le traitement des données à caractère personnel lorsqu'il existe un déséquilibre manifeste entre la personne concernée et le responsable du traitement, en particulier lorsque ce dernier est une autorité publique et qu'il est improbable que le consentement ait été donné librement au vu de toutes les circonstances de cette situation particulière* »

422 Décision du 18 août 2019 de la Datainspektionen : « Inom skolområdet är det tydligt att elva står i beroendeställning till skolan vad klassificering, studiemedel, utbildning och därmed möjlighet till framtida arbete eller fortatta studier », Traduit par nous

423 Voy. *supra.*

424 Skollag (2010:800),https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk forfattningssamling/skollag-2010800_sfs-2010-800

qu'il existe une base juridique pour administrer la fréquentation scolaire des élèves [...] il n'y a pas de soutien juridique explicite pour mener à bien la tâche par le biais du traitement de données personnelles sensibles ou par d'autres moyens plus menaçants pour la vie privée. » Le fait que l'affaire ne concernât qu'un faible nombre de lycéens n'emporta pas de conséquence quant à l'atteinte grave portée à l'intégrité des enfants.

En définitive, conformément au principe de minimisation des données, le régulateur considéra que le contrôle des présences peut être effectué d'une autre manière qui ne nuit pas à la vie privée des personnes concernées. Le dispositif de reconnaissance faciale mis en place lors de cette expérimentation était ainsi considéré comme disproportionné par rapport à sa finalité.

BIBLIOGRAPHIE

I. Législation

- *Skollag(2010:800),*https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/skollag-2010800_sfs-2010-800
- *Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning,* https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2018218-med-kompletterande-bestammelser_sfs-2018-218
- *Brottsdatalag (2018:1177),* https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/brottsdatalag-20181177_sfs-2018-1177
- *SFS 2018:1249 Lag om ändring i brottsdatalagen (2018:1177),* https://www.lagboken.se/Lagboken/sfs/sfs/2018/1200-1299/d_3284308-sfs-2018_1249-lag-om-andring-i-brottsdatalagen-2018_1177
- *Lag (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område,* https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-20181693-om-polisens-behandling-av_sfs-2018-1693
- *SFS 2019:1188 Lag om ändring i lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område,* https://www.lagboken.se/Lagboken/sfs/sfs/2019/1100-1199/d_3806074-sfs-2019_1188-lag-om-andring-i-lagen-2018_1693-om-polisens-behandling-av-personuppgifter-inom

II. Prise de position des autorités régulatrices de la protection des données

- *Datainspektionen, "Förhandssamråd om Polismyndighetens planerade pilotverksamhet med biometrisk ansiktsverifiering vid yttre gräns"*, 16 décembre 2019, https://www.datainspektionen.se/globalassets/dokument/ovrigt/forhandssamrad-polisen-ansiktsverifiering-skavsta.pdf
- *Datainspektionen, « Förhandssamråd om Polismyndighetens planerade användning av programvara för ansiktsigenkänning mot signalementsregistret »*, 23 octobre 2019, https://www.datainspektionen.se/globalassets/dokument/ovrigt/2019-10-23-polisen-forhandssamrad.pdf
- *Datainspektionen, « Lagändring krävs för att polisen ska kunna utföra testverksamhet av ansiktsverifiering på flygplats »*, 17 décembre 2019, https://www.datainspektionen.se/nyheter/lagandring-kravs-for-att-polisen-ska-kunna-utfora-testverksamhet-av-ansiktsverifiering-pa-flygplats/
- *Datainspektionen, « Polisen får använda ansiktsigenkänning för att utreda brott »*, 24 octobre 2019, https://www.datainspektionen.se/nyheter/polisen-far-anvanda-ansiktsigenkanning-for-att-utreda-brott/
- *Datainspektionen, « Tillsyn enligt EU:s dataskyddsförordning 2016/679 – ansiktsigenkänning för närvarokontroll av elever »*, 20 août 2019, https://www.datainspektionen.se/globalassets/dokument/beslut/beslut-ansiktsigenkanning-for-narvarokontroll-av-elever-dnr-di-2019-2221.pdf

III. Presse numérique

- Burt C, « Police facial recognition off in Orlando, on in Netherlands and considered in Sweden » [en ligne], *BiometricUpdate*, 22, juillet 2019, [consulté le 30/01/2020], https://www.biometricupdate.com/201907/police-facial-recognition-off-in-orlando-on-in-netherlands-and-considered-in-sweden

- Lefaix E, « RGPD : Première amende pour la Suède après avoir utilisé la reconnaissance faciale dans un lycée » [en ligne], *SiècleDigital*, 28 août 2019, [consulté le 01/02/2020], https://siecledigital.fr/2019/08/28/amende-suede-reconnaissance-faciale-rgpd/
- Hoy M, « Police Use of Facial Recognition Tech Approved in Sweden » [en ligne], *Bloomberg Law*, 25 octobre 2019, [consulté en ligne le 30/01/2020, https://news.bloomberglaw.com/privacy-and-data-security/police-use-of-facial recognition-tech-approved-in-sweden
- Pascu L, « VeriScan biometrics surpass 1M air passengers processed as Japan, Jamaica, Sweden add checks » [en ligne], *BiometricUpdate.com*, 17 décembre 2019, [consulté le 30/01/2020], https://www.biometricupdate.com/201912/veriscan-biometrics-surpass-1m-air-passengers-processed-as-japan-jamaica-sweden-add-checks

Autres

I. Danemark

Le Danemark ne dispose pas de législation spécifique à la reconnaissance faciale. Comme dans les autres États européens, il dispose d'une législation relative à la protection des données - le *Danish Data Protection Act* - du 25 mai 2018[425], qui complète la mise en œuvre du RGPD.

L'expérimentation conduite dans le stade de Brøndby a été, pour l'autorité compétente en matière de protection des données - la *Datatilsynet*[426], - l'occasion de préciser sa position. Dans une décision de mai 2019[427], elle autorisa le club de Brøndbyernes IF Fodbold A / S - à traiter des données biométriques à l'aide de la reconnaissance faciale. La technologie permet d'identifier, dès l'entrée du stade, les personnes soumises à une interdiction d'accès.

Le traitement dont est responsable le Club de football est un traitement de données à caractère personnel couvert par l'article 9 du RGPD et par l'article 7 du *Danish Data Protection Act*. S'agissant d'une entreprise privée le traitement est soumis à l'autorisation de l'autorité de contrôle, qui peut, le cas échéant fixer une série de conditions pour que le traitement soit licite.

En l'espèce, la Datatilsynet a fourni neuf précisions sur le traitement dont sera responsable le Club de football, parmi lesquelles:

- La liste des personnes n'ayant pas accès au stade doit être faite sur une base factuelle et proportionnée ;
- Les données personnelles traitées dans le cadre du système de reconnaissance faciale qui n'entraînent pas de correspondance avec les informations de la liste interne de Brøndby IF ne peuvent pas être stockées ;
- Les données personnelles traitées dans le cadre du système de reconnaissance faciale doivent être transportées et stockées cryptées sur le serveur avec des algorithmes de cryptage à jour et largement reconnus ;
- Les données personnelles traitées doivent être stockées sur un serveur distinct et ne doivent pas être exposées à internet ;
- Brøndby IF doit organiser le contrôle d'accès du personnel ainsi que l'utilisation de l'authentification à deux facteurs lors de la connexion au système ;
- Les données personnelles traitées dans le cadre du système de reconnaissance faciale qui aboutissent à une correspondance avec des informations de la liste interne de Brøndby IF doivent être supprimées immédiatement après tout match ;
- Brøndby IF est tenu à une obligation d'information lorsque le traitement automatique des données biométriques est en cours.

D'autres expérimentations sont parallèlement envisagées dans ce pays ; le chef de la police de Copenhague a exprimé la volonté d'équiper les forces de police de dispositifs de reconnaissance faciale[428]. Selon lui, la technologie présenterait un "avantage considérable" dans le cadre des enquêtes.

---

425 *Danish Data Protection Act* du 25 mai 2018, https://www.datatilsynet.dk/media/6894/danish-data-protection-act.pdf

426 Le « Datatilsynet » est une autorité centrale indépendante qui supervise le respect des règles de protection des données. Elle conseille, guide, traite les réclamations et effectue des inspections auprès des autorités et des entreprises : https://www.datatilsynet.dk/om-datatilsynet/

427 Datatilsynet, "Tilladelse til behandling af biometriske data ved brug af automatisk ansigtsgenkendelse ved indgange på Brøndby Stadion", 24 mai 2019, https://www.datatilsynet.dk/tilsyn-og-afgoerelser/tilladelser/2019/maj/tilladelse-til-behandling-af-biometriske-data-ved-brug-af-automatisk-ansigtsgenkendelse-ved-indgange-paa-broendby-stadion/?fbclid=IwAR3DPah3y6uNZ-VqmW_gA_wJoW2NBSmMgHb-wPdniO-H4mhuTFNkDzeajMo

428 J.B Nielsen, "København Politi: Vi vil gerne bruge ansigtsgenkendelse på borgerne" [en ligne], *Berlingske*,23 octobre 2019, [consulté le 27/01/2020], https://www.berlingske.dk/samfund/koebenhavns-politi-vi-vil-gerne-bruge-ansigtsgenkendelse-paa-borgerne

II. Finlande

La Finlande a conduit une expérimentation intéressante dans le cadre aéroportuaire. Du 2 au 23 mai 2017, un essai de la reconnaissance faciale a été réalisé par la compagnie aérienne Finnair lors de l'enregistrement des passagers à l'aéroport d'Helsinki. Un panel de 1000 personnes a été mobilisé. Les personnes volontaires ont envoyé leur photo via une application de test au niveau système de reconnaissance faciale mis en place. Il s'agissait ensuite de passer par des comptoirs *ad hoc* afin que le système de reconnaissance faciale puisse s'activer. Un agent déterminait si la reconnaissance avait ou non fonctionnée. Le système a été fourni par la société « Futurice », dont la technologie repose sur l'utilisation de logiciels et de cloud. Le responsable de projet, Tuğberk Duman, indique que « *cela nous permet d'identifier au vol les passagers enregistrés, sans avoir à stocker des images. Ce test fournit des informations utiles sur l'utilisation de cette solution dans les environnements avec des flux de clients importants et des besoins accentués de sécurité* ».

L'objectif affiché de ces expérimentations est l'augmentation de la sécurité et de la rapidité des flux des voyageurs au moment des contrôles[429]. Cette expérience avait déjà été testée au poste de contrôle de sécurité des employés. Cette dernière avait produit des résultats définis comme assez encourageants pour que l'expérience soit reconduite au sein de l'aéroport. L'utilisation d'un cloud peut interroger quant à la sécurité des données qui vont être utilisées, cependant le responsable de projet indique que ces données ne seront pas stockées afin de les protéger au maximum.

III. Slovénie

La Slovénie a également conduit une expérimentation aéroportuaire de la technologie. En 2019, l'aéroport de Ljubljana a autorisé la mise en place d'un embarquement biométrique avec reconnaissance faciale. Ce service est prodigué par la société Amadeus. Cette dernière collabore avec la société Gemalto qui lui fournit les caméras ainsi que les logiciels de biométrie.

Les passagers volontaires se servent d'un téléphone fourni par la société qui dispose de l'application mobile nécessaire au bon fonctionnement du système. Ensuite les volontaires (ici, 175 passagers) enregistrent sur un serveur distant via cette application, une photo de leur passeport ou de leur carte d'identité ainsi qu'un selfie.

La photo renseignée par les passagers est ensuite comparée à celle capturée par la caméra lors du passage de la personne à la porte d'embarquement. Le but est de valider l'identité et le statut de vol du volontaire. Si la comparaison des deux photos est un succès, un message des serveurs biométriques est envoyé au système sur place -la borne avec la caméra- pour que le message «Please proceed » s'affiche et que la personne soit autorisée à embarquer. Afin de garantir la conformité au RGPD, les données biométriques sont systématiquement supprimées au bout de 48 heures. Le consentement des passagers est le fondement juridique sur lequel est fondé l'usage de la technologie.

La société Amadeus estime que l'embarquement pour chaque passager dure approximativement deux secondes (environ 75% de diminution de la durée) contre 10 secondes habituellement[430]. L'expérience aurait enregistré un taux de correspondance effective de 98%.

---

429 « *La technologie de reconnaissance faciale pourrait offrir des possibilités de fluidifier le processus de départ du point de vue du client, et éliminer la nécessité d'avoir une carte d'embarquement* » selon Sari Nevanlinna, le directeur de l'expérience au sol.

F. DUCLOS, « Finnair aussi teste la reconnaissance faciale » [en ligne], *Air Journal*, 2 mai 2017, [consulté le 30/01/2020], https://www.air-journal.fr/2017-05-02-finnair-aussi-teste-la-reconnaissance-faciale-5181002.html

430 R. MORAES, « Amadeus teste l'embarquement a reconnaissance faciale à l'aéroport de Ljubljana » [en ligne], *Air Journal*, 19 mai 2019, [consulté le 30/01/2020], https://www.air-journal.fr/2019-05-19-amadeus-teste-lembarquement-a-reconnaissance-facile-a-laeroport-de-ljubljana-5212514.html

BIBLIOGRAPHIE

I. Législation

- *Danish Data Protection Act* du 25 mai 2018, consulté en ligne le 25.02.2020 à l'adresse suivante : https://www.datatilsynet.dk/media/6894/danish-data-protection-act.pdf

II. Prise de position des autorités régulatrices de la protection des données

- DATATILSYNET, *Tilladelse til behandling af biometriske data ved brug af automatisk ansigtsgenkendelse ved indgange på Brøndby Stadion,* 24 mai 2019, *consulté en ligne le 25.02.2020 à l'adresse suivante : https://www.datatilsynet.dk/tilsyn-og-afgoerelser/tilladelser/2019/maj/tilladelse-til-behandling-af-biometriske-data-ved-brug-af-automatisk-ansigtsgenkendelse-ved-indgange-paa-broendby-stadion/?fbclid=IwAR3DPah3y6uNZ-VqmW_gA_wJoW2NBSmMgHb-wPdniO-H4mhuTFNkDzeajMo*

III. Presse numérique

- DUCLOS F., « Finnair aussi teste la reconnaissance faciale », *Air Journal*, 2 mai 2017, consulté en ligne le 30.01.2020 à l'adresse suivante : https://www.air-journal.fr/2017-05-02-finnair-aussi-teste-la-reconnaissance-faciale-5181002.html

- MORAES R., « Amadeus teste l'embarquement a reconnaissance faciale à l'aéroport de Ljubljana », *Air Journal*, 19 mai 2019, consulté en ligne le 30.01.2020 à l'adresse suivante : https://www.air-journal.fr/2019-05-19-amadeus-teste-lembarquement-a-reconnaissance-facile-a-laeroport-de-ljubljana-5212514.html

- MURAINE L. « La reconnaissance faciale comme nouveau mode de paiement », *Sciences et Avenir*, 19 juillet 2013, consulté en ligne le 30.01.2020 à l'adresse suivante : https://www.sciencesetavenir.fr/high-tech/la-reconnaissance-faciale-comme-nouveau-mode-de-paiement_35424

- NIELSEN J.B, *Københavns Politi: Vi vil gerne bruge ansigtsgenkendelse på borgerne, Berlingske,* 23 octobre 2019, consulté en ligne le 27.01.2020 à l'adresse suivante : https://www.berlingske.dk/samfund/koebenhavns-politi-vi-vil-gerne-bruge-ansigtsgenkendelse-paa-borgerne

- SAMAMA P., « La reconnaissance faciale testée en Europe par PayPal et Uniqul », *01Net*, 13 août 2013, consulté en ligne le 30.01.2020 à l'adresse suivante : https://www.01net.com/actualites/la-reconnaissance-faciale-testee-en-europe-par-paypal-et-uniqul-601163.html

- UNIQL, vidéo de promotion, « Machine inspired by Magic TM » , Youtube, 14 juillet 2013, consulté en ligne le 25.02.2020 à l'adresse suivante : https://www.youtube.com/watch?v=xDO4hdfY11U&feature=youtu.be


UNIVERSITÉ
CÔTE D'AZUR
DL4T
UCA DEEP LAW FOR TECH

INVESTISSEMENTS D'AVENIR
INITIATIVE D'EXCELLENCE

UCA
J.E.D.I.
UNIVERSITÉ CÔTE D'AZUR

Fablex