

LIVRE BLANC POUR L'OBSERVATOIRE DE L'ÉTHIQUE PUBLIQUE

Surveiller les foules

POUR UN ENCADREMENT DES IA
« PHYSIOGNOMONIQUES »



Sous la direction de C. Lequesne Roth
Avec les contributions de C. Lequesne Roth
et J. Keller

SOUS LA DIRECTION de

Caroline Lequesne – Roth

Maître de conférences HDR en Droit public à l'Université Côte d'Azur, membre du GREDEG (CNRS – UMR 7321)

AVEC LES CONTRIBUTIONS de



Caroline Lequesne – Roth

Maître de conférences HDR en Droit public à l'Université Côte d'Azur, membre du GREDEG (CNRS – UMR 7321)



Jonathan Keller

Ingénieur de recherche (Département SES, Institut Mines Telecom), chef de projet du Projet Living Lab 5G mené en partenariat avec la SNCF, Nokia et Orange et financé par la Banque Publique d'Investissement (BPI)

EN BREF

Le présent rapport intéresse le recours aux technologies d'identification par les forces de police dans les espaces accessibles au public : reconnaissance faciale, vidéosurveillance intelligente, systèmes de police « prédictive ». Un des points de convergence technologique tient dans la mobilisation de techniques dites d'IA « physiognomoniques ». La physiognomonie promet de déduire des caractéristiques physiques d'une personne, certains traits de caractère. Cette pseudo science - héritée de l'Antiquité et promue de manière controversée au 19^e siècle - connaît aujourd'hui une résurgence au travers du déploiement de l'intelligence artificielle. Nous désignons comme IA physiognomoniques les systèmes développés au service de l'identification des personnes dangereuses, au départ du gabarit d'un visage (reconnaissance faciale) ou du gabarit standard d'une personne considérée comme dangereuse (reconnaissance comportementale et émotionnelle). La présente étude dresse un état des lieux des usages de ces technologies, en analyse les risques et le régime juridique applicable, puis formule, en conclusion, des propositions visant à en combler les lacunes. Pour renforcer la démocratie technologique, l'étude plaide en faveur d'une stricte restriction des usages et de l'adoption d'un régime de redevabilité adapté.

REMERCIEMENTS

Les auteurs tiennent à remercier l'équipe de l'Observatoire de l'Ethique Publique pour son écoute, les échanges qui ont entouré la réalisation du présent Libre Blanc et le travail éditorial réalisé.

SOMMAIRE

Remerciements	7
Sommaire	9
Liste des abréviations	11
INTRODUCTION. Des jeux olympiques au « panopticon »	13
I. Technologies de surveillance, IA physiognomonique : qu'est-ce à dire ?	17
A. Reconnaissance faciale	17
B. Vidéo surveillance dite « intelligente »	22
C. L'hypothèse de l'IA physiognomonique	29
II. De la maturité technologique à l'acceptabilité sociale : les risques de l'IA physiognomonique	31
A. Dysfonctionnements technologiques et état de droit	32
1. <i>Les atteintes aux droits fondamentaux résultant des biais algorithmiques</i>	32
2. <i>Sécurité des données et souveraineté numérique</i>	38
B. Technologies de surveillance contre les libertés	42
1. <i>Surveillance généralisée et atteinte à la vie privée</i>	42
2. <i>Liberté d'expression, de croyance et d'assemblée et le <u>chilling effect</u></i>	44
III. Les lacunes des régimes applicables aux technologies physiognomoniques	47
A. L'absence de fondements légaux adaptés	48
1. <i>Les fondements communs aux régimes administratifs et judiciaire</i>	49
2. <i>Les fondements propres au régime administratif</i>	54
B. Les garanties incertaines du régime en vigueur	56
1. <i>Les garanties dues au titre de la protection des données</i>	56
2. <i>Les garanties liées au responsable du traitement</i>	61
3. <i>Les garanties techniques et architecturales</i>	65
4. <i>Le contrôle humain</i>	67
5. <i>La garantie des droits des personnes concernées</i>	69
C. Les pièges de l'instrumentalisation démocratique : le cas des expérimentations	73
IV. Pour un régime de redevabilité adapté	77
1. <i>Limitier strictement les usages de l'IA physiognomonique</i>	78
2. <i>Identifier les autorités compétentes</i>	79
3. <i>Autoriser et contrôler</i>	81
4. <i>Reconnaître la normative des actes numériques</i>	83
5. <i>Renforcer le devoir d'information</i>	83
6. <i>Approfondir les analyses d'impact</i>	84
7. <i>S'interroger quant au régime de consentement</i>	85

LISTE DES ABRÉVIATIONS

AIA	Artificial Intelligence Act
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Informations
CASS. CRIM.	Chambre Criminelle de la Cour de Cassation
CNCDH	Commission Nationale Consultative des Droits de l'Homme
CE	Conseil d'Etat
CEDH	Cour Européenne des Droits de l'Homme
CEPD/EDPB	Comité Européen pour la Protection des Données
CJUE	Cour de Justice de l'Union Européenne
CNIL	Commission Nationale de l'Informatique et des Libertés
Cons. Const.	Conseil Constitutionnel
DINUM	Direction INterministérielle du NUMérique
EWCA	England and Wales Court of Appeal
JORF	Journal Officiel de la République Française
LINC	Laboratoire d'Innovation Numérique de la CNIL
RGPD	Règlement Général pour la Protection des Données
TA	Tribunal Administratif

INTRODUCTION

Des Jeux olympiques au « panopticon »

-1. Alors que la France se prépare à l'organisation de plusieurs événements sportifs de dimension mondiale, les enjeux sécuritaires sont de nouveau au cœur du débat public, avec, en ligne de mire, les espoirs que laissent miroiter les technologies. Vidéoprotection par système d'intelligence artificielle, reconnaissance faciale, repérage automatique des objets abandonnés, surveillance des foules, reconnaissance des comportements suspects : autant d'outils sur lesquels la bonne marche des Jeux olympiques 2024 (JO) pourrait reposer.

Précisons que l'intérêt pour ces technologies ne relève nullement de la contingence. Si, historiquement, les événements sportifs et culturels sont l'occasion d'inscrire dans le long cours les technologies de surveillance¹, ils produisent davantage l'effet d'un catalyseur dans une dynamique déjà engagée et connue. À l'échelon européen, ces technologies suscitent, depuis plusieurs années, le plus vif intérêt, comme en témoigne la multiplication des expérimentations technologiques sécuritaires sur le territoire². La frontière européenne en constitue une autre manifestation : elle se caractérise comme une frontière « technologiquement » surveillée, au péril des droits fondamentaux des migrants, nous y reviendrons. Si le discours national français se veut « prudent », le gouvernement, se faisant écho des forces de l'ordre, se montre également favorable à l'équipement technologique des polices et de la gendarmerie³.

-2. La présente étude s'intéresse au déploiement des technologies de surveillance permettant d'identifier les individus dans les espaces accessibles au public. Comme nous le verrons, l'identification couvre un large spectre de finalités et ne se résume pas seulement à

¹ Voir en ce sens les travaux de références de K. HAGGERTY et C.J. BENNETT, *Security games: Surveillance and control at mega-events*, Routledge, 2012.

² *New Surveillance Technologies in Public Spaces - Challenges and Perspectives for European Law at the Example of Facial Recognition*, Report for The Urban Agenda, EUROPEAN COMMISSION, April 2021, 96 p., [en ligne](#).

³ En ce sens, les lignes directrices tracées par le Livre Blanc de la sécurité intérieure, 16 novembre 2020, [en ligne](#).

l'établissement d'un lien entre un individu et son état civil. L'identification technologique peut également être catégorielle, et conduire à des rapprochements entre un individu et certaines caractéristiques établies ou supposées. Nous privilégions aussi une approche plus large que celle qui consisterait à se concentrer sur la seule technologie de reconnaissance faciale, en abordant ce que nous désignerons comme les intelligences artificielles (ci-après IA) « physiognomoniques » : des systèmes permettant l'identification des individus au départ de leurs données biométriques. Ils recouvrent, comme nous l'étudierons, les technologies de reconnaissance faciale, émotionnelle, comportementale et de nombreux dispositifs entourant la vidéo surveillance dite « intelligente ». Le choix d'aborder ces technologies dans un même mouvement, et sous l'empire d'une catégorie commune, procède de motifs d'ordre divers. D'une part, d'un point de vue technologique, ces systèmes ne se distinguent pas tant en termes de nature qu'en termes de degrés ; ils recourent aux mêmes dispositifs techniques et répondent le plus souvent aux mêmes finalités sécuritaires. D'autre part, ce choix permet d'envisager plus « sereinement » la course législative. La dynamique d'innovation est aujourd'hui si forte que raisonner depuis technologies elles-mêmes condui(rai)t inévitablement à l'obsolescence programmée de la loi. Poser les jalons du point de vue des finalités et des effets paraît à cet égard plus pérenne. Cela permet en outre, et enfin, d'anticiper certaines mains-d'œuvre légistiques conduisant in fine à affaiblir nos droits fondamentaux. L'exemple de l'organisation des JO est à cet égard éloquent. Les craintes que suscite, à raison, l'implémentation de la reconnaissance faciale dans l'opinion publique ont conduit le législateur à en écarter, pour l'heure, l'usage. Par un effet de comparaison supposément « minimisateur », il lui préfère aujourd'hui la vidéosurveillance intelligente, considérée comme moins attentatoire aux libertés fondamentales. Une analyse des risques soulevés par ces systèmes permettra d'établir qu'il n'en est rien : l'identification d'une personne comme d'un comportement peut conduire à des effets discriminants de même nature. Les enjeux se posent en termes de reconnaissance et d'identité bien au-delà d'une technologie particulière.

3-. Pour conduire l'analyse, nous procéderons en quatre temps. La première partie définit les notions et concepts clefs des technologies de surveillance physiognomoniques. Nous nous attachons à distinguer les systèmes de reconnaissance faciale, émotionnelle et comportementale pour mettre en évidence leur nature commune (I). La seconde partie

permet d'envisager les risques soulevés par cette catégorie particulière de technologies au regard des usages déployés. Il s'agit à la fois de cartographier et d'évaluer les pratiques à l'aune des droits fondamentaux d'une part, des risques proprement techniques de l'autre (II). La troisième partie propose une analyse du régime juridique applicable à ces technologies. Nous montrons à cette occasion les lacunes des bases légales fondant leur déploiement et les faiblesses du régime de redevabilité auxquelles les responsables de traitements auront peine à se conformer en raison de leur nature. Pour ce faire, nous nous appuyons sur la législation européenne déjà en vigueur (RGPD et directive police justice) et discutons des propositions législatives en cours (proposition de la loi d'expérimentation pour les JO 2024 et de la proposition de règlement européen sur l'intelligence artificielle) (III). La quatrième partie envisage enfin une série de propositions plaidant en faveur de l'adoption d'un régime de redevabilité idoine (IV).



I. Technologies de surveillance, IA physiognomonique : qu'est-ce à dire ?

-4. Les technologies de surveillance appellent à un examen particulièrement minutieux à l'aune du risque qu'elles font peser sur nos régimes de libertés : les atteintes se comprennent dans les mécaniques, les usages et les effets. Nous nous attacherons en premier lieu à définir deux technologies phares dont le déploiement alimente aujourd'hui le débat public européen : la reconnaissance faciale (A) et la vidéosurveillance intelligente (B). En tant qu'outil de surveillance des individus et des foules, ces deux technologies convergent dans une fonctionnalité essentielle : la catégorisation et la hiérarchisation des individus dans les espaces accessibles au public. Elles procèdent en ce sens d'une même « famille » de systèmes : celle des intelligences artificielles physiognomoniques (C).

A. Reconnaissance faciale

-5. Selon les termes de la CNIL, la reconnaissance faciale est une technique permettant d'authentifier ou d'identifier une personne à partir des traits de son visage⁴. En d'autres termes, la technologie permet de « reconnaître » un individu grâce à ses données biométriques.

⁴ CNIL, *Reconnaissance faciale*, [en ligne](#).

Plusieurs éléments de définition méritent d'être précisés.

-6. Premièrement, la distinction opérée entre authentification et identification. Celle-ci est importante en ce qu'elle appelle des traitements de données fonctionnellement différents. L'**authentification** consiste à vérifier qu'une personne est bien celle qu'elle prétend être. Parmi les usages les plus fréquents dans les espaces accessibles au public, les contrôles d'accès aux frontières, utilisés dans les aéroports : le système vérifie que la personne que se présente correspond au profil biométrique enregistré dans les papiers d'identité présentés. Les systèmes d'authentification ne requièrent pas la constitution préalable d'une base de données pour l'opération de reconnaissance. Tel n'est pas le cas de l'**identification** qui a précisément pour objet de vérifier qu'un visage présenté correspond à l'un des modèles contenus dans une base de données. Tandis que l'authentification s'opère dans des environnements contrôlés⁵, l'identification est le plus souvent réalisée à distance. La proposition de règlement européen sur l'intelligence artificielle⁶ (ci-après AIA) porte ainsi une attention particulière à ces dispositifs désignés comme des « systèmes d'identification biométrique à distance ». Ils permettent d'identifier des personnes physiques « sans leur participation active », par la comparaison des données biométriques captées avec celles contenues dans un référentiel donné⁷. Un système de reconnaissance faciale peut en outre être mobilisé en temps réel ou a posteriori. Bien que la distinction soit, à juste titre, critiquée⁸, elle sert communément à décrire deux usages. Tout d'abord, l'usage de la reconnaissance faciale pour la surveillance en continu - notamment dans le cadre d'événements culturels ou sportifs. Ensuite, l'usage de la technologie dans le cadre de procédures, notamment pour l'identification de personne sur une scène de crime.

À des fins d'encadrement, certains chercheurs invitent en outre à introduire une subdivision entre **systèmes d'identification biométrique ciblée** et **non ciblée**. Le premier consiste à scanner

⁵ Nous désignons par contrôlés les espaces dont la lumière, la distance – facilitant voire permettant la captation de l'image « à comparer » - sont maîtrisées.

⁶ Proposition de Règlement du Parlement Européen et du Conseil Établissant des Règles Harmonisées Concernant l'intelligence artificielle (Législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union, COM(2021) 206 final (« AIA » par la suite).

⁷ Article 3 (36) de l'AIA.

⁸ Voir en ce sens les analyses du CDT Europe, qui appelle à minimiser la différence pour éviter son instrumentalisation. Un décalage de quelques secondes serait différé et pourrait bénéficier d'un régime moins protecteur au terme de l'AIA alors que cela consisterait en une même opération pour un même résultat. CDT Europe, CDT Facial recognition briefing Paper, February 2023, [en ligne](#).

une foule indéterminée pour retrouver une personne précise, tandis que le second ne procède qu'au départ d'une seule image, visant une seule personne. Nous verrons, en effet, que le risque d'atteinte aux droits et libertés, présent dans les deux cas, est plus significatif – voire inacceptable – dans le premier.

-7. Deuxièmement, la particularité des systèmes de reconnaissance faciale tient dans le traitement de **données biométriques**, qui constituent des données sensibles et bénéficient à ce titre d'une protection renforcée⁹.

Le Règlement général sur la protection des données (ci-après RGPD) et la directive police justice définissent ces dernières comme « les 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 »¹⁰. Il en résulte que les éléments constitutifs d'une donnée biométrique sont l'existence d'un traitement et la finalité de reconnaissance d'un individu. Ces notions appellent quelques précisions.

-7a. Sur le traitement, tout d'abord. Le RGPD retient une définition relativement extensive de la notion en définissant celle-ci comme « toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction »¹¹. Toutefois, le considérant (51) de ce même texte introduit un point d'incertitude qui mériterait d'être éclairci. Il précise que le traitement des photographies « ne devrait pas systématiquement être considéré comme constituant un traitement de catégories particulières de données à caractère personnel, étant donné que celles-ci ne relèvent de la définition de données biométriques que lorsqu'elles sont traitées selon un mode technique

⁹ Article 9 du Règlement général sur la protection des données (UE) 2016/679 du 27 avril 2016 (RGPD) et article 10 de la directive police justice (UE) 2016/680 du 27 avril 2016 (« **directive police justice** » par la suite).

¹⁰ Article 4 (14) du RGPD ; article 2(13) de la directive police justice.

¹¹ Article 4 (2) du RGPD.

spécifique permettant l'identification ou l'authentification unique d'une personne physique ». En suivant ce raisonnement, les photographies « brutes » qui ne font pas l'objet d'une opération de « reconnaissance » ne rentrent pas dans la catégorie des données biométriques. Aussi, gouvernements et entreprises pourraient constituer des bases de données d'images faciales ne bénéficiant pas de la protection due aux données sensibles. Cette lacune s'inscrit en faux avec les exigences de la Cour européenne des droits de l'homme¹² et mériterait, comme le préconise de E. KINDT¹³, de revoir la définition des données biométriques.

-7b. Sur la destination du traitement ensuite : la reconnaissance. Le Comité européen de la protection des données (European Data Protection Board, ci-après CEPD), apporte, dans ses récentes directives, des précisions intéressantes. Peut être compris, au terme de la reconnaissance, le simple fait de suivre dans une foule une personne sans que le lien avec son identité civile ne soit nécessairement établi¹⁴. Cela permet d'inclure un large spectre de traitements, permettant, a contrario de nos précédentes remarques, une protection plus extensive.

-8. Plusieurs rapports ont d'ores et déjà permis de dresser un état des lieux des usages de la reconnaissance faciale dans les espaces accessibles aux publics en Europe¹⁵.

Nous retenons que la reconnaissance faciale y a principalement été déployée à titre expérimental ; le contexte politique et l'environnement légal que nous étudierons ci-après constituent, pour l'heure encore, un obstacle à son déploiement pérenne. Il explique notamment le recul de la France, qui avait annoncé l'adoption de la technologie pour les JO 2024, avant d'y renoncer¹⁶. Huit secteurs sont plus particulièrement concernés. Comme l'indique le schéma ci-dessous, ils regroupent le domaine des transports (secteur aérien, gare, métro, ports), largement majoritaire, puis la surveillance d'événements (culturel ou sportif),

¹² Voir en ce sens nos travaux, « De la fin de l'anonymat : reconnaissance faciale et droit à la vie privée », *Dalloz IP/IT*, Juin 2021, pp. 308-313.

¹³ KINDT E., *A First Attempt at Regulating Biometric Data in the European Union*, AI NOW, *Regulating Biometrics: Global Approaches and Urgent Questions*, 2020, p.66, [en ligne](#).

¹⁴ EDPB, *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement*, Version 1.0, adopted on 12 May 2022, Point 10, p.7, [en ligne](#).

¹⁵ C. LEQUESNE ROTH, (Dir) *La reconnaissance faciale dans l'espace – Une cartographie juridique européenne*, *Fablex DL4T*, Avril 2020, 128 p. *New Surveillance Technologies in Public* op cit.

¹⁶ « JO 2024 : la reconnaissance faciale ne sera pas expérimentée durant les Jeux », *Le Monde*, 23 novembre 2022.

les écoles et les centres commerciaux. Ces tendances semblent se confirmer comme en témoigne l'intérêt croissant pour la technologie en Espagne¹⁷, en Suisse¹⁸ ou au Royaume-Uni¹⁹. Ajoutons enfin qu'à date, la majorité des usages procèdent d'opérations d'authentification.

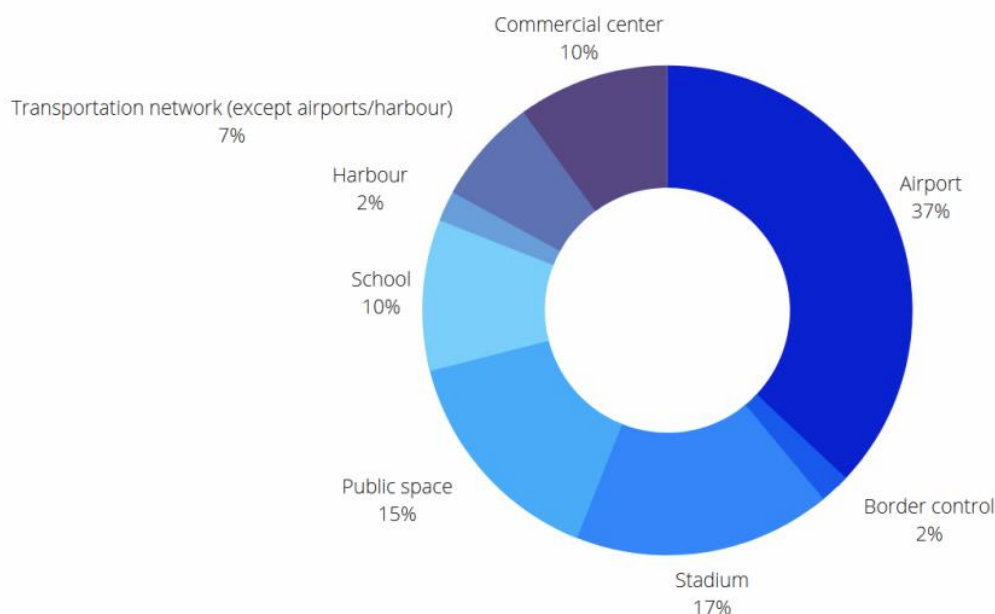


Figure 1 : les usages sectoriels de la reconnaissance faciale

Source : *New Surveillance Technologies in Public Spaces*, op cit, p. 32.

-9. En France, la reconnaissance faciale dans les espaces accessibles au public a fait l'objet de trois expérimentations, qui n'ont pas été pérennisées. La première s'est tenue à Nice, en 2018. La police expérimentait la technologie à l'occasion du Carnaval, sur la base du consentement de plusieurs agents administratifs que le logiciel devait retrouver dans la foule²⁰. Elle devait encore être expérimentée dans deux lycées de la région Provence Alpes Côte d'Azur ; un recours a toutefois mis un terme à l'expérimentation pour défaut de base légale²¹. Enfin, si ces expérimentations demeurent relativement marginales, le recours à la reconnaissance faciale a

¹⁷ Développement de la reconnaissance faciale annoncée dans le métro barcelonais pour lutter contre le vandalisme et les graffitis. « Le métro de Barcelone utilisera la reconnaissance faciale », *Equinox*, 17 février 2023, [en ligne](#).

¹⁸ « Les CFF veulent équiper leurs gares de caméras à reconnaissance faciale », *RTS*, 18 février 2023, [en ligne](#).

¹⁹ Voir en ce sens le dernier rapport de l'autorité compétente, *Biometrics and Surveillance Camera Commissioner, Report 2021 to 2022*, 9 February 2023, [en ligne](#).

²⁰ *New Surveillance Technologies in Public Spaces*, op cit., pp. 44-46.

²¹ *TA Marseille*, 27 février 2020, n°1901249.

posteriori est institué. Le décret relatif traitement des antécédents judiciaires (TAJ)²² autorise la police à recourir à la reconnaissance faciale dans le cadre d'enquêtes ou de simples contrôles d'identité. Selon les derniers chiffres disponibles, 375 747 recherches auraient été effectuées en 2019, 207 584 entre le 1er janvier et le 17 juin 2020²³. Ainsi, le déploiement de la reconnaissance faciale est limité par son caractère intrusif évident. Toutefois, l'avancée spectaculaire des applications sécuritaires de l'intelligence artificielle ont trouvé un moyen détourné pour continuer à évoluer : les caméras dites « intelligentes ».

B. Vidéo surveillance dite « intelligente »

-10. La vidéosurveillance dite « intelligente » ou « augmentée » regroupe quant à elle plusieurs techniques d'analyse automatisée d'images à partir de caméras vidéo. Avant d'en préciser la nature, rappelons qu'en l'espèce, nous nous intéressons uniquement à ses usages (et caractéristiques techniques) dans le cadre de la surveillance des espaces accessibles au public. Comme le rapporte la CNIL – et en témoigne l'exemple des Jeux olympiques 2024 que nous développerons ci-après – la demande des autorités publiques est aujourd'hui particulièrement forte en ce domaine²⁴.

-11. Florent CASTAGNINO précise qu'elle répond à deux principales fonctionnalités : un travail de repérage et un travail d'évaluation²⁵. Grâce aux logiciels d'intelligence artificielle, ces systèmes doivent théoriquement effectuer une catégorisation permettant, dans un second temps, l'adoption de mesures ou l'orientation des agents sur le terrain. La vidéosurveillance intelligente est à cet égard promue, par l'industrie, comme un remède à l'inefficacité de la vidéosurveillance : en optimisant le travail des agents, elle « décuplerait la capacité de contrôle

²² Décret n° 2012-652 du 4 mai 2012 relatif traitement des antécédents judiciaires.

²³ ASSEMBLEE NATIONALE, [Avis n°3404](#), Tome VII Sécurités.

²⁴ « Le souhait des autorités publiques de s'équiper de dispositifs toujours plus perfectionnés pour l'exercice de leur mission de sauvegarde de l'ordre public, de protection des populations ou encore d'aménagement des territoires, ou celui des commerçants de vouloir optimiser le pilotage de leur activité et la rentabilité de celle-ci, au moyen d'une connaissance encore plus fine des conditions et caractéristiques de fréquentation de leurs espaces de vente », CNIL, Caméras dites « intelligentes » ou « augmentées » dans les espaces publics, Juillet 2022, [en ligne](#).

²⁵ F. CASTAGNINO, « Rendre « intelligentes » les caméras : déplacement du travail des opérateurs de vidéosurveillance et redéfinition du soupçon », Sciences Po Cities and Digital Technology Chair Working Paper, N°05/2019.

policier »²⁶. Si cette efficacité est contestable, nous y reviendrons, catégorisation et gestion constituent les deux composantes fonctionnelles de la vidéosurveillance intelligente.

Contrairement à la reconnaissance faciale, ces systèmes ne visent pas nécessairement l'identification d'une personne, voire les personnes elles-mêmes²⁷. La loi d'expérimentation en cours d'adoption au Parlement français permet de le comprendre. L'article 7 du projet de loi relatif aux jeux olympiques et paralympiques de 2024 prévoit d'autoriser, à titre expérimental jusqu'au 30 juin 2025, le traitement d'images collectées au moyen de systèmes de vidéoprotection par un système d'intelligence artificielle. Les systèmes opéreront selon la double finalité évoquée : il s'agira de « détecter, en temps réel, des événements prédéterminés susceptibles de présenter ou de révéler ces risques et de les signaler en vue de la mise en œuvre des mesures nécessaires, par les services de la police et de la gendarmerie nationale, les services d'incendie et de secours, les services de police municipale et les services internes de sécurité de la SNCF et de la Régie autonome des transports parisiens ». Le texte précise encore que la détection et le signalement porteront sur « des événements anormaux, des mouvements de foule, des objets abandonnés ou des situations présumant la commission d'infractions ». Le spectre de la vidéosurveillance intelligente couvre ici la surveillance des objets, des foules et des comportements.

-12. Bien que la **reconnaissance émotionnelle et comportementale** ne soit pas expressément mentionnée, elle semble en effet constituer un préalable – ou une composante – de l'anticipation « d'infractions » et, dans certains cas, « d'événements anormaux » auxquels il est fait référence. Selon certains travaux récents²⁸, aux relents d'eugénisme²⁹, la criminalité pourrait en effet être détectée dans les visages ou les comportements. L'AIA propose aussi de définir un « système de reconnaissance des émotions », comme « un système d'IA permettant la reconnaissance ou la déduction des émotions ou des intentions de personnes physiques sur la base de leurs données biométriques »³⁰. Le repérage d'une intentionnalité - aussi abscons

²⁶ T. JUSQUIAME, « Les cuisines de la surveillance automatisée », *Le Monde diplomatique*, février 2023.

²⁷ Bien que la reconnaissance dite comportementale ou émotionnelle repose sur des données biométriques.

²⁸ La plus retentissante d'entre elles, au regard des réponses et critiques qu'elle a suscitées, est celle de X. WU and X. ZHANG, *Automated inference on criminality using face images*, 2016, 2016, [en ligne](#). Ces chercheurs soutiennent que la criminalité est une caractéristique innée et revêt une dimension biologique que les IA seraient aujourd'hui en mesure de détecter.

²⁹ Nous reviendrons sur les critiques suscitées par ces travaux dans la seconde partie de notre étude.

³⁰ Article 3(34) de l'AIA.

soit-il – fait écho aux dispositions nationales françaises. En l’absence de dispositions plus spécifiques, la vidéosurveillance telle que décrite pourrait également s’inscrire dans les systèmes dits de « catégorisation biométrique » que l’AIA propose de définir comme des systèmes d’IA destinés à « affecter des personnes physiques à des catégories spécifiques sur la base de leurs données biométriques »³¹. Notons que la proposition initiale mentionnait, au titre des catégories « le sexe, l’âge, la couleur des cheveux, la couleur des yeux, les tatouages, l’origine ethnique ou l’orientation sexuelle ou politique ». Le déploiement de technologie de surveillance sur la base d’une telle catégorisation paraît toutefois totalement contraire à nos droits fondamentaux, et inconcevable dans un régime démocratique.

-13. Les usages de la vidéosurveillance intelligente n’ont pas, à notre connaissance, fait l’objet de recensement exhaustif. Celui-ci est d’autant plus délicat que ces technologies recouvrent une « multitude de cas d’usage envisageables » selon les termes de la CNIL³².

-14. **À l’échelon européen**, les outils de police prédictive font l’objet de nombreuses réflexions et expérimentations³³. Les études recensent plusieurs solutions « d’anticipation » des infractions développées en interne par les polices européennes : CAS (Crime Anticipation System), système adopté par la police d’Amsterdam depuis 2015, « Precobs », qui équipe certaines polices allemandes et suisses, ou « Keycrime » à Milan³⁴. Le plus souvent toutefois, les polices en Europe ont recours à des outils déployés par de grands opérateurs technologiques à l’instar de Palantir. L’actualité allemande en témoigne : jusqu’à la condamnation de la Cour Constitutionnelle en février 2023, les forces de police des Länder de la Hesse et de Hambourg avaient recours aux algorithmes de cette société pour prévenir les infractions et assurer, sur la base des données collectées, la gestion de son personnel³⁵.

³¹ Article 3(35) de l’AIA.

³² CNIL, *Caméras dites « intelligentes » ou « augmentées » dans les espaces publics*, op cit.

³³ Voir par exemple : F. JANSEN, *Data driven policing in the context of Europe*, Data Justice Lab, 2018, [en ligne](#); P. WILLIAMS and E. KIND, *Data-driven Policing: The hardwiring of discriminatory policing practices across Europe*, Project Report, European Network Against Racism (ENAR), 2019, [en ligne](#); W. HARDYNS, A. RUMMENS, “Predictive Policing as a New Tool for Law Enforcement? Recent Developments and Challenges”, *Eur J Crim Policy Res* 24, 201–218 (2018), [en ligne](#).

³⁴ *New Surveillance Technologies in Public Spaces*, op. cit., p.41.

³⁵ *Cour Constitutionnelle allemande, 16 février 2023, 1 BvR 1547/19, 1 BvR 2634/20. Pour une analyse relative aux outils de Palantir en cause dans cette affaire : « Germany Raises Red Flags About Palantir’s Big Data Dragnet », The Wired, 17 février 2023, [en ligne](#).*

Par ailleurs, le contrôle de la frontière européenne constitue un terrain de déploiement privilégié des technologies de surveillance en général, de la vidéosurveillance augmentée en particulier³⁶. Plusieurs projets de reconnaissance émotionnelle ont été mis en œuvre³⁷. Le plus emblématique est le système « iBorderCtr », financé par la Commission européenne et expérimenté aux frontières grecque, hongroise et lettone entre 2016 et 2019³⁸. Ce système, voué à accélérer les contrôles, subordonnait le passage aux frontières à l'évaluation émotionnelle des voyageurs. En amont de leur arrivée, les passagers transmettaient par voie électronique copie de leurs papiers d'identité. À l'arrivée, le système interrogeait les personnes identifiées par le truchement d'un haut-parleur, et analysait la fiabilité de leurs réponses. Le système, dont les détails techniques sont demeurés largement inconnus³⁹, était supposément capable de discerner, parmi trente-huit « micromouvements », les déclarations mensongères d'un individu. Si le système jugeait qu'un voyageur mentait, il lui délivrait un « jeton » à haut risque. Le voyageur se voyait alors conduit dans la file où les gardes-frontières récupéraient ses données biométriques : empreintes digitales et des veines de la main, image faciale. Si le système ne détectait aucun mensonge, le voyageur pouvait emprunter la file à « bas risque » où les contrôles étaient restreints.

-15. À l'échelon national, le déploiement d'outils de police prédictive est connu, et a fait l'objet de divers travaux⁴⁰. Deux dynamiques semblent à l'œuvre dans le secteur. D'une part, des outils ont été développés, expérimentés et pérennisés à l'échelon central. Tel est le cas du système « Paved »⁴¹, un logiciel d'aide à l'analyse décisionnelle dans la lutte contre la délinquance, élaboré par la gendarmerie nationale. Testé dans onze départements français, son usage a été élargi à l'ensemble du territoire en septembre 2018. Il permet une cartographie des cambriolages et atteintes aux véhicules afin d'orienter l'action des militaires

³⁶ Sur la question, voy. l'étude très complète de D. OZKUL, *"Automating Immigration and Asylum: The Uses of New Technologies in Migration and Asylum Governance in Europe"*, Oxford: Refugee Studies Centre, University of Oxford, 2023.

³⁷ Ibidem, p.26.

³⁸ Devenu par la suite iCROSS A hauteur de 4 501 877€, Projet n°: 700626, <https://cordis.europa.eu/project/id/700626/fr>

³⁹ Aux termes d'un recours porté devant la Cour de Justice de l'Union qui n'accédait pas à la demande de communication du défendeur. Voir infra.

⁴⁰ Mentionnons à titre principal, C. CASTETS-RENARD, P. BESSE, J.-M. LOUBES et L. PERRUSSEL, *Encadrement des risques techniques et juridiques des activités de police prédictive, Rapport 2019 CHEMI, Ministère de l'intérieur, 12 Juillet 2019, 85 p.*

⁴¹ Ibidem, p. 31.

sur le terrain⁴². À l'échelon des territoires, les villes ont conclu divers marchés publics « d'analyse statistique et cartographique de la délinquance ». Nombre d'entre elles semblent privilégier le système « Map Révélation » proposé par l'entreprise angevine « Sûreté Globale »⁴³. Selon le site Internet de l'entreprise, le logiciel « fournit des analyses prédictives, graphiques et géographiques » renseignées par des « semis de points composés (...) de faits de délinquance, incidents »⁴⁴. Le site indique encore que le logiciel « révèle les lieux et les moments importants », « prédit les occurrences » et permet aux patrouilles de police d'ajuster « en fonction des besoins la stratégie en matière de police de proximité »⁴⁵.

Concernant plus spécifiquement la « vidéosurveillance automatisée », la cartographie dressée par l'initiative Technopolice⁴⁶ s'avère très instructive. D'après les données recueillies, la « vidéosurveillance automatisée » aurait d'ores et déjà été déployée et/ou expérimentée dans une trentaine de villes.

⁴² « Il s'agit (...) de donner aux gendarmes la possibilité de placer un militaire dans les zones où une situation est susceptible d'éclater, soit pour éviter sa survenance, soit pour intervenir le plus vite possible ». *Rapp. Sénat n° 621, 9 juill. 2020, p. 36.*

⁴³ *Initiative regroupant des associations et collectifs militants pour lutter contre la surveillance technologique. TECHNOPOLICE, La police prédictive progresse en France. Exigeons son interdiction !, 23 juillet 2020, [en ligne](https://technopolice.fr/villes/).*

⁴⁴ *Ibidem.*

⁴⁵ *Ibidem.*

⁴⁶ <https://technopolice.fr/villes/>

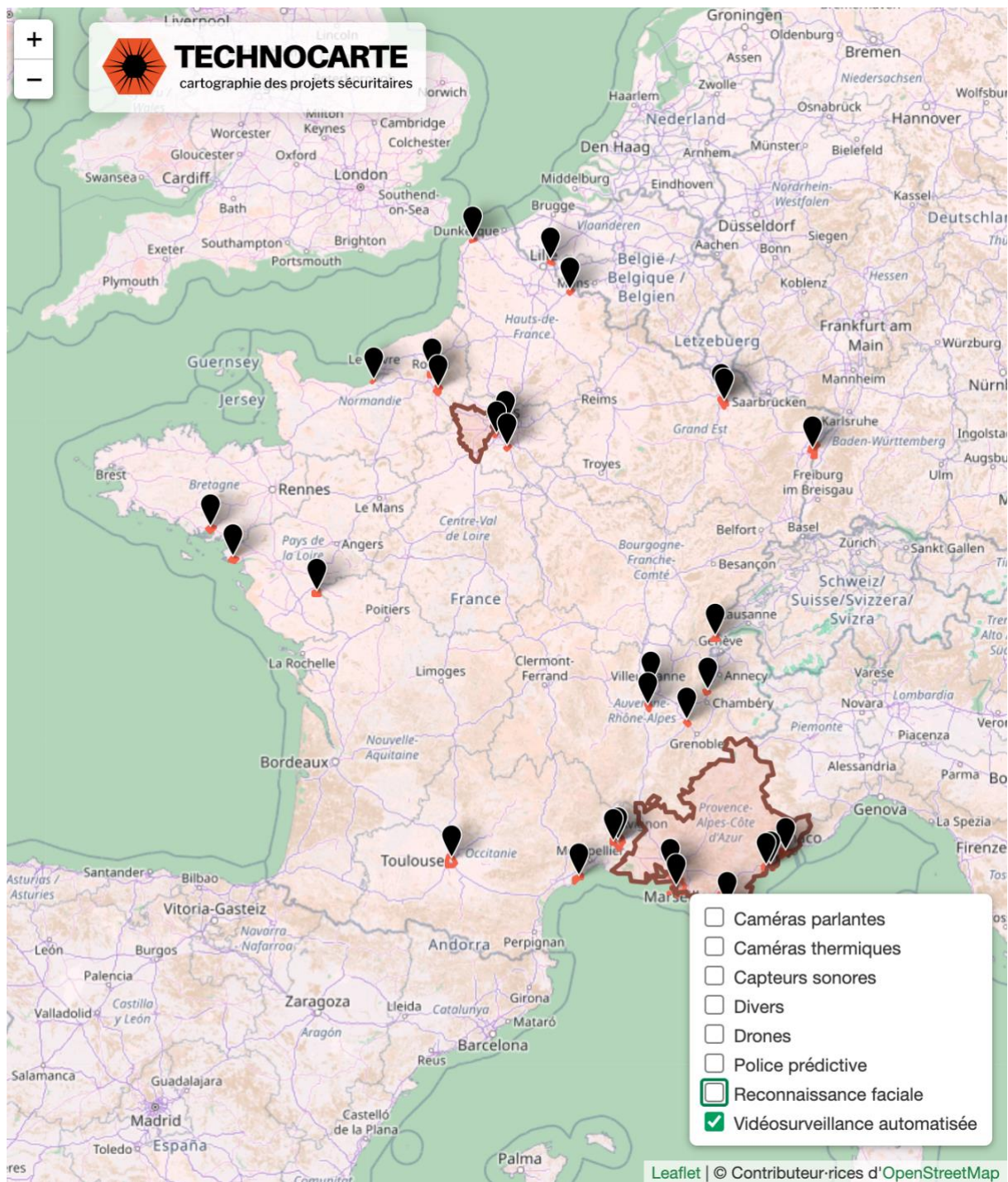


Figure 2 : Cartographie des usages de la vidéosurveillance automatisée.

Source : [Technopolice](#), 2023.

Parmi elles, trente-cinq villes⁴⁷ auraient adopté le logiciel d'analyse « Briefcam », dont la promesse marketing est de « de visionner 1h de vidéo en 1 minute » et « faire des recherches par attributs » (taille, couleur ou vitesse) »⁴⁸.

La ville de Nice s'illustre particulièrement par la multiplicité de ses expérimentations, effectives ou avortées⁴⁹. Outre le projet d'expérimentation « Safe City » (2018-2021) – destiné à « développer les nouveaux algorithmes d'analyse et de corrélation permettant de mieux comprendre une situation et de développer des capacités prédictives »⁵⁰ – mentionnons la détection automatique des « stationnements anarchiques » sur les pistes cyclables : « les caméras de vidéosurveillance de Nice détecteront 'en temps réel, tout véhicule, deux roues, camion et voiture, présent sur ces voies plus d'une minute' avant d'envoyer une alerte au centre de supervision urbain afin de verbaliser le conducteur d'une amende de 135 euros »⁵¹. En outre, le centre de supervision urbain disposerait d'ores et déjà « d'outils d'analyse comme la détection de maraudage, de regroupement de foule, de détection de colis suspects. De nouveaux algorithmes d'analyse d'objets sont en fonction comme la reconnaissance automatique de forme de véhicule ou de piéton »⁵².

La vidéosurveillance embrasse ainsi un large spectre d'usages et de technologies. *Dès lors qu'elles visent à identifier un comportement ou une catégorie d'individus, ces technologies s'inscrivent, comme la reconnaissance faciale, dans la catégorie des technologies d'identification que nous désignerons ci-après comme les « IA physiognomoniques ».*

⁴⁷ Selon l'entreprise. Les usages identifiés concernent les villes de Roubaix, Vannes, Vitrolles, Nice, Vienne, Woippy, La Baule, Gex, Moirans, Vaulx en Velin, A Caveirac (dans le Gard), Nîmes, Aix-les-bains et Deauville.

⁴⁸ TECHNOLICE, Briefcam, [en ligne](#).

⁴⁹ Dont certaines ont été avortées, à l'instar de l'introduction de la reconnaissance émotionnelle dans le réseau de tramway annoncé en 2019. « Un logiciel pour décoder les émotions des usagers du tramway de Nice », France Bleu, 4 janvier 2019, [en ligne](#).

⁵⁰ Convention d'expérimentation, de mise à disposition et de démonstration, pour le Projet d'expérimentation « Safe City », conclu entre Thales Communications & Security SAS, la ville de Nice et la Métropole Nice Côte d'Azur, référence SIX/TCS/PRS/DJC/CZ/2018-029 V2.0, pp. 23-24.

⁵¹ « Nice : Les stationnements sur les pistes cyclables seront désormais vidéo verbalisés », 20 minutes, 2 décembre 2022, [en ligne](#).

⁵² TECHNOLICE, Nice, [en ligne](#). Voir également le Cahier des clauses techniques particulières du contrat de fournitures de la Métropole Nice Côte d'Azur [mise en ligne](#) grâce à la rédaction de Nextimpact.

C. L'hypothèse de l'IA physiognomonique

-16. Que partagent la reconnaissance faciale et la vidéosurveillance intelligente et que nous enseigne leur étude concomitante dans la surveillance des individus ? Le premier élément de réponse est assurément technique : le fonctionnement de leurs systèmes respectifs repose sur l'existence ou l'implémentation d'un réseau de caméras de vidéosurveillance dont les images, les données, sont traitées par des logiciels d'intelligence artificielle. Nous soutenons que cette filiation est encore politique et sociale. Traduction de relations de pouvoir singulières, il importe d'analyser pour prendre la pleine mesure de l'adoption de ces systèmes dans nos régimes démocratiques. Dans les espaces accessibles au public, la reconnaissance faciale et la vidéosurveillance appliquée aux individus⁵³ ont toutes deux vocations à identifier et catégoriser ces derniers au départ de leurs données biométriques qui incluent, rappelons-le, les données comportementales. *Elles consistent ainsi à plaquer des « modèles » sur des individus pour en déduire les comportements à adopter : intervenir, sanctionner, protéger.* Ces modèles, qui résultent de la seule « corporéité », recèlent ainsi une vérité sur le monde : cet individu est dangereux, suspect, vulnérable. La reconnaissance faciale ne s'écarte pas du schéma. Elle constitue le degré de granularité ultime du modèle. En effet, la technologie demeure mobilisée à de mêmes fins : identifier un individu, en l'espèce grâce à *son* modèle de données unique (le gabarit), en raison de sa dangerosité (effective ou potentielle) ou de sa vulnérabilité. Plusieurs travaux outre-Atlantique⁵⁴ y voient une réminiscence de la physiognomonie à laquelle l'intelligence artificielle donnerait aujourd'hui une force applicative à échelle. Cette pseudoscience, dont on attribue communément l'origine à Aristote⁵⁵, proposait d'analyser et de classifier les humains à partir de ses caractéristiques physiques. Elle connut dans l'histoire différentes variantes : la métoposcopie (analyse de la personnalité à partir du dessin des lignes, rides et marques du front), la chiromancie (des lignes de la main), puis la phrénologie (analyse de l'architecture du crâne) qui marqua son renouveau au 19^{ème} siècle⁵⁶. Les systèmes de reconnaissance faciale et émotionnelle fonctionnent sur le même

⁵³ Par opposition à la surveillance des seuls objets.

⁵⁴ L. STARK and J. HUTSON, "Physiognomic Artificial Intelligence", 32 Fordham Intell. Prop. Media & Ent. L.J. 922, 2022 [en ligne](#); C. STINSON, "The Dark Past of Algorithms That Associate Appearance and Criminality", American Scientist, Jan-Feb 2021, Vol 109, n°1, p.26, [en ligne](#); C.E. THOMSON, "Phrenology is here to stay", Medium, 11 février 2021, [en ligne](#).

⁵⁵ A.-M. LECOQ, Physiognomonie, Encyclopédie Universalis en ligne.

⁵⁶ Au travers de l'ouvrage de Lavater, qui inspira à son tour les travaux de Franz Josef Gall.

principe, en automatisant les catégorisations et autres hiérarchisations sur le fondement des modèles physiognomoniques. Ces modèles, en forme de catégories descriptives, n'offrent toutefois qu'une vision partielle – et le plus souvent partielle, nous le verrons – de la réalité. Ils contribuent sinon à la réification de l'homme à sa réduction simpliste

En réalité, les technologies de surveillance précédemment décrites procèdent d'une même famille de systèmes d'intelligence artificielle : les IA « physiognomoniques ». Cette notion invite à les appréhender et à les encadrer dans un même mouvement : reconnaissance faciale et comportementale (au travers de la vidéo surveillance) en constituent deux variantes qui ne se distinguent pas tant en termes de degré que de nature.



II. De la maturité technologique à l'acceptabilité sociale : les risques de l'IA physiognomonique

-17. Dans le débat public, la question de l'opportunité des usages est souvent envisagée au prisme des dysfonctionnements technologiques. Cette approche n'est pas sans intérêt et mérite en effet que l'on s'y arrête : *comment peut-on admettre que des technologies potentiellement dysfonctionnelles constituent l'une des bases des missions des forces de l'ordre sans entraver nos principes démocratiques ?* Il apparaît toutefois essentiel, à titre prospectif et plus largement éthique, d'appréhender la question de l'acceptabilité sociale et juridique dans une hypothèse fonctionnelle, c'est à dire dans l'hypothèse où elles fonctionneraient sans erreur. En effet, les progrès industriels en matière de recherche et de développement nourrissent la promesse d'une pleine efficacité des systèmes : réduction des biais, systèmes mieux entraînés sur des jeux de données plus large. *Dans cette hypothèse, l'usage de IA physiognomonique entrave-t-elle l'exercice de nos droits ? Pourrait-on soutenir que l'efficacité technologique emporte une mise en conformité au régime de libertés ? Assurément non.*

Seront successivement envisagées les atteintes aux droits fondamentaux résultant des dysfonctionnements de l'IA (A), puis les atteintes résultant des IA elles-mêmes, indépendamment de leur qualité ou efficacité techniques (B).

A. Dysfonctionnements technologiques et État de droit

-18. Depuis 2018, les recherches technologiques dénonçant les dysfonctionnements et autres risques technologiques en matière d'IA physiognomonique ont été nombreuses et largement médiatisées. Elle se concentrent principalement autour de deux critiques : les premières tiennent aux biais et interrogent les droits fondamentaux, plus particulièrement le principe d'égalité et l'exercice du droit au respect de la vie privée (1) ; les secondes concernent la sécurité des systèmes et soulèvent des difficultés sur le terrain de la souveraineté des données (2).

1. Les atteintes aux droits fondamentaux résultant des biais algorithmiques

-19. Un biais se comprend comme une « déviation par rapport à un résultat censé être neutre, loyal ou encore équitable »⁵⁷. On distingue communément deux grandes familles de biais : les biais cognitifs, qui procèdent d'une « une distorsion de la manière dont l'information est traitée par rapport à un comportement rationnel ou à la réalité »⁵⁸ et les biais statistiques, qui correspondent à des biais dans les jeux de données ou des biais de représentativité des différentes « populations » composant la population. Rapportés au traitement algorithmique, les biais dans les systèmes peuvent ainsi résulter de leur modélisation : le choix des critères qui définissent un modèle – tout comme leur pondération et leur pertinence – peut être porteur et générateur de discriminations⁵⁹ ; ils peuvent encore être le fruit de la constitution des bases des données, s'il y a une disproportion manifeste dans la représentation d'un groupe ou que l'annotation est elle-même biaisée⁶⁰. Notons qu'une proportion similaire de représentativité ne garantit pas pour autant une absence de biais. La complexité du modèle peut interpréter

⁵⁷ P. BERTAIL, D. BOUNIE, S. CLEMENÇON, P. WAELEBROECK, *Algorithmes : Biais, Discrimination et Équité*, 2019, [en ligne](#).

⁵⁸ *Ibidem*, p.9.

⁵⁹ J. CHARPENET, C. LEQUESNE ROTH, « Discriminations et biais générés - Les lacunes juridiques de l'audit algorithmique », *Dalloz* 2019, 3 Octobre 2019, n°33/7834, p. 1852.

⁶⁰ *Ibidem*.

un résultat statistique correct mais entraînant des décisions individuelles désastreuses. L'exemple le plus connu est l'aide à la décision judiciaire aux États-Unis où, nonobstant l'équilibre de représentativité entre les « populations » noires et blanches, le modèle n'en conclut pas moins que la première population soit plus à même de récidiver⁶¹.

-20. Les technologies de surveillance physiognomoniques sont particulièrement exposées aux biais de la seconde catégorie, liés aux données. Les travaux pionniers de Joy BUOLAMWINI et Timmit GEBRU ont dès 2018 mis en évidence les dysfonctionnements qu'ils engendraient en matière de reconnaissance faciale⁶². En raison de jeux de données d'entraînement peu représentatifs, les erreurs sont statistiquement plus fréquentes sur les personnes de couleurs et les femmes⁶³, créant un fort risque de discriminations dans les usages. Les récents travaux confirment ces constats : bien que le taux d'erreur des systèmes développés soit tendanciuellement à la baisse, il demeure important, notamment sur les populations sous-représentées⁶⁴. Ces mêmes biais ont été observés en matière de reconnaissance émotionnelle dont les dysfonctionnements seraient accrus sur les personnes de couleur⁶⁵. Des biais de nature sociale ont également été inférés dans une étude allemande, qui a démontré que les résultats du système variaient en fonction des habits portés ou des lunettes⁶⁶.

-21. L'IA physiognomonique n'est pas pour autant exempte de biais proprement cognitifs. La probité des études scientifiques relatives à la catégorisation des comportements et des émotions humains est particulièrement contestée. « Pseudo-science »⁶⁷, elle reposerait sur « des inférences simplistes et inexactes, ne pouvant assurer de manière fiable les fonctions qui

⁶¹ K. HAO, *AI is sending people to jail—and getting it wrong*, Technology review 2019, [lien](#).

⁶² 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.

⁶³ Selon cette même étude, le taux d'erreur s'élevait à 35% pour les femmes de peau noire contre 0,8% pour les hommes de peau claire.

⁶⁴ Les biais inhérents aux systèmes de reconnaissance faciale les travaux pionniers de

⁶⁵ L. RHUE, « Racial Influence on Automated Perceptions of Emotions », SSRN, November 9, 2018, [en ligne](#).

⁶⁶ Dans le cadre d'entretien d'embauche. Voir le site dédié à l'étude : [Bayerischer Rundfunk](#).

⁶⁷ Selon le psychologue américain, pionnier dans l'étude des émotions dans leurs relations aux expressions faciales. Propos rapporté dans l'article du Financial Times, « Emotion recognition: can AI detect human feelings from a face? », 12 mai 2021, [en ligne](#).

lui sont dévolues »⁶⁸. En l'absence de fondement scientifique concret⁶⁹, ces systèmes reposent inévitablement sur la compréhension subjective du monde de leurs auteurs. L'étude de WU et ZANG, déjà citée, postule ainsi que la criminalité est innée et procède de paramètres biologiques à l'exclusion de toute autre considération, notamment sociale. Leurs travaux sont d'ailleurs inspirés du mathématicien eugéniste Karl PEARSON qui leur confèrent une base mathématique biaisée. Dans le même sens, il est intéressant d'observer que la phrénologie en particulier a été au fondement de discours politiques diamétralement opposée, justifiant tour à tour les discours abolitionnistes et les apologies de l'esclavagisme⁷⁰.

-22. L'Institut national des standards et des technologies américains (U.S. National Institute of Standards and technology (NIST) fait encore mention d'un autre type de biais, lié aux deux précédents : les biais d'usages, qui procèdent des pratiques. Il indique que les problèmes liés aux biais techniques précédemment évoqués constitue la partie immergée de l'iceberg, et invite à une approche sociotechnique⁷¹. Dans le cas de l'IA physiognomonique, cela crée un risque supplémentaire : que les outils renforcent les biais existants dans la société (racisme) en leur offrant une base pseudo scientifique. En d'autres termes, les biais technologiques renforcent risquent de renforcer les biais sociaux existants conduisant au profilage raciste, communément désigné comme le « délit de faciès ».

⁶⁸ L. F. BARRETT, R. ADOLPHS, S. MARSELLA, A.M. MARTINEZ, & S.D. POLLAK, "Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements". *Psychological Science in the Public Interest*, 20(1), 2019, pp. 1–68. [En ligne](#).

⁶⁹ C. STINSON, "The Dark Past of Algorithms That Associate Appearance and Criminality", déjà citée.

⁷⁰ C.E. THOMSON, "Phrenology is here to stay", précédemment citée.

⁷¹ Qui engage également la lutte contre les biais dans les usages, en formant les agents notamment. Il s'agit d'éviter que les biais techniques ne renforcent les biais sociaux. NIST Special Publication 1270, *Towards a Standard for Identifying and Managing Bias in Artificial Intelligence*, Mars 2002, [en ligne](#).

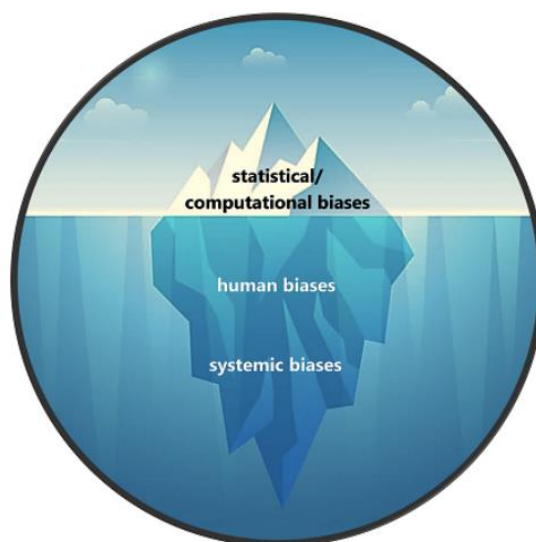


Figure 3 : le défi de la gestion des biais algorithmiques

Source : NIST, 2022

-23. L'ensemble de ces biais est à l'origine de dysfonctionnements potentiels ou effectifs – à l'instar des arrestations erronées⁷² –, qui font courir divers risques en termes de droits fondamentaux.

-24. Risque d'atteinte à l'interdiction de la discrimination et au droit à l'égalité de traitement.

Dès lors que les erreurs portent plus spécifiquement sur certains publics (personnes de couleur, personnes errantes, personnes victimes de trouble du comportement, etc.), le risque de stigmatisation – et par suite de discrimination – dans les espaces accessibles au public est particulièrement élevé. Le Conseil de l'Europe souligne ainsi l'usage de technologies physiognomoniques dysfonctionnelles constituerait une atteinte à l'article 14 de la Convention européenne des droits de l'homme et au protocole n°12⁷³. Dans le même sens, le Défenseur des droits met en garde contre « le risque majeur de renforcer 'essentialisation' et 'stéréotypes' car le caractère prédictif de l'algorithme est basé sur le comportement ou les

⁷² Aux États-Unis, où ces technologies sont plus développées, des procédures faisant suite à des arrestations fondées sur des faux-positifs sont pendantes. Ces faux concernent systématiquement des hommes de peau noire. "How wrongful arrests based on AI derailed 3 men's lives", Wired, 7 mars 2022, [en ligne](#).

⁷³ Vers une régulation des systèmes d'IA, Compilation de contributions préparée par le Secrétariat du CAHAI, Etude de Conseil de l'Europe DGI (2020)16, Décembre 2020, [en ligne](#). Egalement : F.Z.BORGESIU, Discrimination, intelligence artificielle et décisions algorithmiques, Conseil de l'Europe, 2018, [en ligne](#) ; EQUINET, Regulating for Equal AI : a new role for equality bodies, 2020, [en ligne](#).

caractéristiques homogénéisées de groupes »⁷⁴. Ces systèmes risquent, selon lui, « de renforcer les discriminations en leur donnant une apparence d'objectivité »⁷⁵. Il insiste en outre particulièrement sur les erreurs engendrées par les IA physiognomoniques : « si les taux d'erreur restent importants pour certaines catégories de personnes protégées par le droit de la non-discrimination, elles seront lésées et devront systématiquement prendre la voie alternative (qui, de fait, ne sera plus vraiment alternative) »⁷⁶. ***Les biais des données de la reconnaissance faciale sont donc susceptibles de générer des discriminations de certaines populations vulnérables.***

-25. Risque d'atteinte à la dignité de la personne humaine. En dépit de son caractère polysémique et bien souvent mystérieux⁷⁷, la dignité humaine est aujourd'hui abondamment mobilisée pour élaborer l'encadrement des intelligences artificielles⁷⁸. Constitutionnellement et conventionnellement consacrée, elle constitue toutefois un principe menacé comme l'a rappelé dans un communiqué récent, le Haut-Commissaire de l'ONU aux droits de l'Homme, Volker TÜRK⁷⁹. L'étude de la jurisprudence européenne montre que la dignité humaine peut être affectée lorsque les IA renforcent des contextes de discrimination⁸⁰. On peut craindre, à cet égard, des atteintes concernant les publics vulnérables. La détection du maraudage en constitue un bon exemple. Rappelons que cette fonctionnalité est prévue dans les outils de police prédictive de certaines collectivités. Or, comme le dénonce les associations de défense des libertés, cette détection pourrait aisément conduire à une « chasse aux personnes mendiant »⁸¹. ***De même, les systèmes étant relativement indifférents aux contextes, ils pourraient détecter comme anormaux des comportements résultant de handicaps.*** De récentes

⁷⁴ DEFENSEUR DES DROIT, *Algorithmes : prévenir l'automatisation des discriminations*, 2020, [en ligne](#), p.6.

⁷⁵ *Ibidem*.

⁷⁶ DEFENSEUR DES DROIT, *Technologies biométriques : l'impératif respect des droits fondamentaux*, 2021, [en ligne](#). Voir également : CNIL et DEFENSEUR DES DROIT, *Comment permettre à l'homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle*, Décembre 2017, [en ligne](#).

⁷⁷ C. GREWE, « La dignité de la personne humaine dans la jurisprudence de la Cour européenne des droits de l'homme », *Revue générale du droit, Etudes et réflexions* 2014, numéro 3, [en ligne](#).

⁷⁸ G. LE MOLI, « Intelligence artificielle vs dignité humaine : quand la sous-performance humaine est légalement requise », *RED*, 2022/1 (N° 4), p. 122-127, [en ligne](#).

⁷⁹ « Human agency, human dignity and all human rights are at serious risk », Comment by UN High Commissioner for Human Rights Volker Türk on advances in artificial intelligence 18 February 2023, [en ligne](#).

⁸⁰ G. LE MOLI, « Intelligence artificielle vs dignité humaine : quand la sous-performance humaine est légalement requise », *op cit*.

⁸¹ LA QUADRATURE DU NET, *Mobilisation générale contre la légalisation de la vidéosurveillance automatisée*, 5 janvier 2023, [en ligne](#).

études redoutent à cet égard les effets de ces systèmes sur les publics autistes⁸². Le Défenseur des droits a appelé à la vigilance⁸³, de même que le Contrôleur européen de la protection des données et le Comité européen de la protection des données à l'occasion d'un avis conjoint⁸⁴. L'atteinte au droit à la dignité est également constituée par l'immixtion de l'État dans la vie privée de ses nationaux.

-26. Risque d'atteinte au droit à la vie privée. Au regard de leur nature intrinsèquement intrusive, le déploiement d'outils dysfonctionnels interroge sur le terrain du droit à la vie privée. Rappelons en effet que ces systèmes mobilisent et traitent parmi les données les plus sensibles qui soient : les données biométriques. Les technologies de surveillance ont fait l'objet de quelques recours, sur ce fondement, devant la Cour Européenne des Droits de l'Homme. Celle-ci admet, de manière constante, les atteintes à la vie privée sous réserve de leur nécessité, légitimité et proportionnalité. Dans l'affaire Olsson c/ Suède, elle établit notamment que la notion de nécessité implique « une ingérence fondée sur un besoin social impérieux et notamment proportionnée au but légitime recherché »⁸⁵. Peut-on admettre que des systèmes largement dysfonctionnels et biaisés relèvent d'un besoin social impérieux ? Que l'atteinte soit proportionnée quand les systèmes font peser de forts risques de discrimination sur (notamment) les publics les plus vulnérables ? Il semble aussi difficile de soutenir qu'en l'état, les IA physiognomoniques répondent aux exigences de la Cour. Nous verrons toutefois que ce raisonnement mérite également d'être conduit indépendamment de l'existence des biais. Envisageons pour l'heure un autre risque lié aux lacunes de ces systèmes : les fuites de données et l'atteinte à la souveraineté numérique.

⁸² Voir par exemple : O. KEYES, "Automating autism: Disability, discourse, and Artificial Intelligence". *Journal of Sociotechnical Critique*, 1(1), (2020), pp. 1-31, [en ligne](#) ;

⁸³ DEFENSEUR DES DROIT, *Technologies biométriques : l'impératif respect des droits fondamentaux*, précédemment cité p. 13.

⁸⁴ Contrôleur européen de la protection des données et le Comité européen de la protection des données, *Avis conjoint 5/2021 sur la proposition de règlement établissant des règles harmonisées sur l'intelligence artificielle*, 18 juin 2021, commentaire C. CRICHTON, *Dalloz Actualité*, 2 juillet 2021.

⁸⁵ CEDH, *Olsson contre Suède*, 24 mars 1988, série A, n° 130 ; J.D.I., 1989, observations P. ROLLAND, p. 799.

2. Sécurité des données et souveraineté numérique

-27. Pour être efficient, le déploiement d'IA physiognomonique suppose *une solidité et une fiabilité d'un réseau de vidéo-caméras d'une part, une sécurisation des données biométriques*, de l'autre. De plus, le programme informatique peut lui-même être sujet à diverses formes d'attaques informatiques⁸⁶. En l'absence de garanties suffisantes à ces différents niveaux, les autorités/entités qui recourent à ces outils s'exposent à des risques majeurs susceptibles d'affecter les personnes ciblées par les systèmes, la sécurité publique et dans certains cas la puissance publique.

-28. Premièrement, lorsque les autorités/entités qui utilisent ces systèmes ne disposent pas de systèmes hardware capables de capturer des images de qualité optimale, la fiabilité des résultats est d'autant incertaine. Dans ce cas, la menace concerne tant les individus ciblés⁸⁷ que la sécurité publique elle-même : d'une part, des personnes peuvent être injustement ciblées ; de l'autre, en tant que partie prenante du dispositif sécuritaire, elle peut affaiblir la garde des forces humaines, qui nourrissent une confiance dans ces dispositifs.

-29. Deuxièmement, les périphériques informatiques – en l'occurrence, les caméras connectées – constituent des points d'entrée pour des attaques informatiques. Dans son panorama de la cybermenace 2022, l'Agence Française de la Sécurité Informatique (ANSSI) rappelle en effet que ces « équipements connectés en permanence (...) fournissent aux attaquants un accès discret et persistant aux réseaux de leurs victimes »⁸⁸. Les conséquences de ces attaques sont potentiellement multiples. Ces équipements exposent les autorités/entités qui les adoptent, comme les personnes concernées par les traitements. Des vols de données biométriques, ont déjà été perpétrés. En août 2019, une faille de sécurité dans une base de données utilisée par des banques, des entrepreneurs de la défense et la police

⁸⁶ LINC, Dossier Sécurité des systèmes d'IA, avril 2022, [lien](#), qui répertorie trois catégories d'attaques des modèles d'intelligence artificielle : les attaques par manipulation, par infection ou par exfiltration. V. également pour les attaques en temps réel sur les modèles d'intelligence artificielle pour la vision, A. Guesmi, K. N. Khasawneh, N. Abu-Ghazaleh and I. Alouani, "ROOM: Adversarial Machine Learning Attacks Under Real-Time Constraints," 2022 International Joint Conference on Neural Networks (IJCNN), Padua, Italy, 2022, pp. 1-10, doi: 10.1109/IJCNN55064.2022.9892437.

⁸⁷ Et renvoie ainsi à nos précédentes analyses sur les systèmes dysfonctionnels.

⁸⁸ ANSSI, Panorama de la cybermenace 2022, [en ligne](#), p.10

métropolitaine britannique a permis d'accéder aux données biométriques de plus d'un million de personnes⁸⁹. La base de données appartenait à la société sud-coréenne Suprema, leader du marché de l'identification biométrique en Europe⁹⁰, au Moyen-Orient et sur le continent africain. En 2020, la base de données controversée Clearview AI, constituée de milliards de données biométriques mises au rebut sur les médias sociaux, a également connu une importante faille de sécurité. Le code source et certaines de ses clés privées sont devenus publiquement accessibles, permettant à quiconque d'accéder à la base de données⁹¹. Des études ont parallèlement démontré que de nombreux systèmes sont vulnérables aux techniques d'usurpation d'identité : des photos, des vidéos, des modèles 3D ou des « deep fakes »⁹² d'un visage peuvent permettre une usurpation⁹³. Des réseaux neuronaux profonds (DNN) peuvent également être trompés par des exemples adverses⁹⁴. Ajoutons plus globalement que l'IA est fondamentalement vulnérable à certains types d'attaques, ce qui questionne la fiabilité des systèmes⁹⁵.

Ces violations sont particulièrement préoccupantes, ces données étant immuables⁹⁶. La CNIL rappelle en ce sens que « toute compromission peut avoir des conséquences graves sur leur vie quotidienne »⁹⁷. De même, le Conseil de l'Europe considère que « [t]oute faille dans la

⁸⁹ TAYLOR J., 'Major breach found in biometrics system used by banks, UK police and defence firms', *The Guardian*, 14 August 2019, [en ligne](#).

⁹⁰ La société fournissait notamment l'Allemagne, la Belgique, et la Finlande Belgique.

⁹¹ WHITTAKER Z., "Security lapse exposed Clearview AI source code", *TechCrunch*, 16 April 2020.

⁹² TARIQ S., JEON S., WOO S. S., Am I a Real or Fake Celebrity? Measuring Commercial Face Recognition Web APIs under Deepfake Impersonation Attack, 2 March 2021.

⁹³ J. K. KHAN and D UPADHYAY, Security issues in face recognition, 5th International Conference - Confluence The Next Generation Information Technology Summit (Confluence), Noida, India, 2014, pp. 719-725. Sudeep S.V.N.V.S., VENKATA KIRAN S., NANDAN D., KUMAR S. "An Overview of Biometrics and Face Spoofing Detection", In: KUMAR A., MOZAR S. (eds) ICCCE 2020. Lecture Notes in Electrical Engineering, vol 698. Springer, Singapore, 2021.

⁹⁴ ALPARSLAN Y., ALPARSLAN K., KEIM-SHENK J., KHADE S., GREENSTADT R., Adversarial Attacks on Convolutional Neural Networks in Facial Recognition Domain, 2021. Egalement: EVTIMOV I. et al, "What if a facial recognition system is too easy to fool? Is Tricking a Robot Hacking?" *Berkeley Technology Law Journal* 34, 2019, p. 891.

⁹⁵ Plusieurs cas d'études ont permis de l'établir : Concernant les plateformes et les enjeux de sécurité (S. Dave et al., "Special Session: Towards an Agile Design Methodology for Efficient, Reliable, and Secure ML Systems," 2022 IEEE 40th VLSI Test Symposium (VTS), San Diego, CA, USA, 2022, pp. 1-14, doi: 10.1109/VTS52500.2021.9794253); les attaques temps-réel sur les modèles d'IA pour la vision (A. Guesmi, K. N. Khasawneh, N. Abu-Ghazaleh and I. Alouani, "ROOM: Adversarial Machine Learning Attacks Under Real-Time Constraints," 2022 International Joint Conference on Neural Networks (IJCNN), Padua, Italy, 2022, pp. 1-10, doi: 10.1109/IJCNN55064.2022.9892437); la vulnérabilité dans le cas de radars intelligents (A. Guesmi and I. Alouani, Adversarial Attack on Radar-based Environment Perception Systems, arXiv:2211.01112v2 [cs.CR] 28 Nov 2022); la vulnérabilité de l'IA dans le cas de conduite autonome (A. Guesmi, M.A. Hanif, I. Alouani and M. Shafique, APARATE: Adaptive Adversarial Patch for CNN-based Monocular Depth Estimation for Autonomous Navigation, arXiv:2303.01351v1 [cs.CV] 2 Mar 2023)

⁹⁶ "If a hacker succeeds in seizing the 35,000 points that make up your face and sells it on the darkweb, it will be almost impossible to recover your digital identity." DECHAUX D., « La vérité sur les failles de la biométrie faciale », *Challenges*, 23 January 2021.

⁹⁷ CNIL, Reconnaissance faciale, pour un débat à la hauteur des enjeux, 2019, [en ligne](#), p10.

sécurité des données peut avoir des conséquences particulièrement graves pour les personnes concernées puisqu'une divulgation non autorisée de données sensibles ne peut être corrigée »⁹⁸. Les attaques peuvent enfin engager les rapports entre États, et menacer la souveraineté nationale. Cela se vérifie particulièrement dans l'hypothèse où les autorités exploitent du matériel informatique étranger. Il est ainsi notoire que les matériels informatiques étasunien⁹⁹ et chinois¹⁰⁰ comportent des « portes dérobées » facilitant l'espionnage par des puissances étrangères. Cet état des lieux se retrouve, malheureusement, également dans les logiciels fournis sous code exécutable. En dehors de l'accès aux serveurs de l'État, ces portes dérobées peuvent surtout influencer les résultats du système de reconnaissance faciale. Elles peuvent injecter ou soustraire des données, et entraîner soit l'identification de fausses menaces soit la mise à l'écart de menaces réelles. Ainsi, l'utilisation de matériel étranger est susceptible de neutraliser la finalité même des systèmes physiognomoniques pour des fins de sécurité de l'État ou de la lutte contre le terrorisme. Dans la première hypothèse, la pratique démontre l'utilisation des systèmes de reconnaissance faciale pour détecter des agents étrangers¹⁰¹. Si les services de renseignement d'États tiers disposent des moyens techniques d'infiltrer les systèmes de reconnaissance faciale déployés par l'État français, ceux-ci peuvent constituer une arme se retournant contre leurs utilisateurs en traquant par exemple des agents français pour déterminer leurs intérêts ou des responsables politiques pour découvrir leur(s) secret(s) et les réemployer à des fins de chantage.

-30. Mentionnons, en dernier lieu, le recours à la sous-traitance privée pour les traitements biométriques. Les ramifications de l'affaire Clearview AI¹⁰² ont mis en évidence les risques soulevés par les usages de son logiciel de reconnaissance en termes de souveraineté. Dans le monde entier, de nombreuses polices ont – ou avaient – sollicité ses services qui offraient un

⁹⁸ COMITE CONSULTATIF DE LA CONVENTION POUR LA PROTECTION DES PERSONNES A L'EGARD DU TRAITEMENT AUTOMATISE DES DONNEES A CARACTERE PERSONNEL, *Lignes directrices pour la reconnaissance faciale*, 28 janvier 2021, T-PD(2020)03rev4, p.12, [en ligne](#).

⁹⁹ En 2016, « Processeur x86 d'Intel, un Backdoor secret et intouchable », GinFO, [en ligne](#), puis de nouveau en 2022 : « Une backdoor cachée dans les derniers processus Intel », Silicon, [en ligne](#).

¹⁰⁰ « Huawei à nouveau accusé d'installer des backdoors », Frandoid, 2021, [en ligne](#).

¹⁰¹ Voir la controverse relative aux usages de la reconnaissance faciale en Ukraine, P. DAVE and J. DASTIN, *Exclusive: Ukraine has started using Clearview AI's facial recognition during war*, 14 mars 2022, Reuters [en ligne](#), « Facial Recognition Goes to War », NYTimes, 7 avril 2022, [en ligne](#).

¹⁰² C. LEQUESNE ROTH, « Mise en demeure de Clearview AI par la CNIL : les jalons d'un combat pour le droit à l'anonymat », Dalloz IP/IT, avril 2022.

accès à l'une des plus vastes bases de données biométriques jamais constituée¹⁰³. L'enquête de l'Organe de contrôle de l'information policière belge, qui fut l'une des plus exhaustive quant aux pratiques policières liées à Clearview, a alerté les autorités belges sur les risques liés à l'extraterritorialité de la société :

*« [L']utilisateur de l'application Clearview n'exerce aucun contrôle sur le traitement des données biométriques. Les photos et les images sont en effet chargées par le biais d'une URL, de sorte que la disponibilité des photos et des images est entièrement confiée à l'entreprise américaine Clearview. Les photos et les images, y compris le traitement biométrique (le template qui contient les données à caractère personnel uniques), **sont envoyées en dehors de l'environnement policier** (et en dehors de l'ordre judiciaire de l'UE) et sont ensuite traitées. L'entité de police qui transmet les photos et les images n'a donc (plus) aucune emprise sur le traitement des données biométriques, ni sur la suite du processus de traitement appliqué par le destinataire. Il est donc clair, et dès lors hautement problématique, **que le service de police qui transmet les photos et les images n'a aucune influence notamment sur le délai de conservation des photos et images, ni sur l'usage commercial qui pourrait potentiellement en être fait par Clearview** »¹⁰⁴.*

En d'autres termes, la collaboration entretenue par les forces de l'ordre avec certains acteurs du secteur privé génère un risque certain de diffusion et de réutilisation incontrôlées des données personnelles collectées lors d'une tâche régalienne.

L'étude que nous avons conduite en 2021 montrait que la plupart des outils de reconnaissance faciale expérimentés ou déployés dans les espaces accessibles au public étaient européens¹⁰⁵, et qu'un effort de déploiement interne était à l'œuvre¹⁰⁶. Toutefois, le secteur de la surveillance, très concurrentiel, se déploie activement sur d'autres continents et les sociétés américaines, chinoises ou encore israéliennes sont parmi les plus compétitives : leur offre fait partie des plus performantes du marché. Cela est en partie lié au fait qu'elles disposent d'importants terrains d'expérimentations à la base de la performance des systèmes. Cette force de frappe étrangère, attractive, appelle à prendre les risques de menace étrangère très au sérieux. Outre une dépendance technologique de prérogatives régaliennes à des

¹⁰³ Ibidem. Selon la presse, la police française est également concernée, bien que nous ne disposions pas d'éléments tangibles permettant de l'établir.

¹⁰⁴ [Rapport DIO21006](#), Février 2022.

¹⁰⁵ *New Surveillance Technologies in Public Spaces*, op cit p. 39.

¹⁰⁶ Ibidem.

technologies étrangères, ces risques constituent indéniablement des menaces aux droits et libertés des citoyens.

B. Technologies de surveillance contre les libertés

-31. Plus fondamentalement, même dans l'hypothèse où la technologie est dite « mûre », la question de l'opportunité de l'usage de l'IA physiognomonique demeure entière. Dans un régime de libertés publiques, peut-on admettre d'être reconnu, catégorisé dans l'espace public par des systèmes prétendument performants ?

Au-delà des considérations sociétales et des convictions personnelles, le droit des libertés fondamentales apporte des réponses connues, tenant au balancement des intérêts. Or proportionnalité et nécessité des usages sont ici questionnables. Nous verrons ainsi que l'usage de technologies physiognomoniques fait peser, indépendamment de leur performance, une menace sur le droit à la vie privée d'une part (1), des libertés d'expression, de croyance et d'assemblée, notamment au travers du chilling effect de l'autre (2).

1. Surveillance généralisée et atteinte à la vie privée

-32. Les juridictions européennes n'ont pas encore eu l'occasion de se prononcer sur la légalité des systèmes de surveillance physiognomoniques. La Cour de justice de l'Union européenne (CJUE) a toutefois été saisie de questions ayant trait à la surveillance de masse des citoyens. Dans l'affaire « Tele2 Sverige », elle a ainsi considéré que la conservation générale et indiscriminée des communications électroniques entraînait une ingérence « particulièrement grave » dans les droits à la vie privée et à la protection des données consacrés par les articles 7 et 8 de la Charte des droits fondamentaux. La surveillance électronique donne à l'individu « le sentiment que sa vie privée fait l'objet d'une surveillance constante »¹⁰⁷. Elle en conclut ainsi que la conservation générale des données relatives au trafic et à la localisation devait

¹⁰⁷ CJUE, *Tele2 Sverige AB contre Post-och telestyrelsen et Secretary of State for the Home Department contre Tom Watson e.a.*, Affaires jointes C-203/15 and C-698/15, §100.

demeurer une exception à la règle¹⁰⁸, et invite les États à limiter la surveillance à ce qui est « strictement nécessaire ».

La jurisprudence postérieure n'a pas remis en cause ces principes, mais en a précisé les exceptions. Les ingérences graves doivent être limitées à des crimes graves et des situations présentant une menace sérieuse et présente (ou prévisible) pour la sécurité nationale. La mesure doit en outre être strictement limitée dans le temps et faire l'objet d'un contrôle de la part des autorités compétentes¹⁰⁹. De surcroît, l'État membre de l'Union européenne ne peut pas invoquer la sécurité nationale, compétence exclusive, pour déroger aux règles fixées dans un domaine de compétence partagée par un règlement européen. Cela signifie donc que l'invocation de la lutte contre le terrorisme ne peut pas déroger au RGPD ou à la directive ePrivacy¹¹⁰.

-33. La Cour européenne des droits de l'homme (CEDH) est parvenue à une conclusion sensiblement similaire concernant l'interception en masse des données de communication (métadonnées)¹¹¹ : de solides garanties contre les abus doivent être fournies par la loi de l'État membre¹¹² par l'inscription d'assurances procédurales¹¹³ et judiciaires¹¹⁴.

-34. Aussi, même dans l'hypothèse improbable du développement d'IA physiognomoniques fonctionnelles, leur déploiement à des fins de surveillance dans les espaces accessibles au public ne pourrait être que restreint au risque de méconnaître les droits à la vie privées. Le

¹⁰⁸ *Ibidem* § 104.

¹⁰⁹ CJUE, Grande chambre, 2 octobre 2018, *Ministerio Fiscal*, C-207/16 ; CJUE, Grande chambre, 6 octobre 2020, *La Quadrature du Net e.a.*, C-511/18 ; CJUE, Gde Ch., 20 septembre 2022, C-339/20 et C-397/20 ; CJUE, 20 septembre 2022, *SpaceNet AG*, C-793/19 et C-794/19.

¹¹⁰ CJUE, gde ch., 6 oct. 2020, *aff. C-511/18, La Quadrature du net*, rappelé par CJUE 2 mars 2021, *aff. C-746/18, H.K./Prokuratuur*.

¹¹¹ CEDH 25 mai 2021, *Big Brother Watch et autres c. Royaume-Uni*, n° 58170/13, 62322/14 et 24960/15 § 424.

¹¹² *Ibidem*, et CEDH 25 mai 2021, *Centrum för Rättvisa c. Suède*, req. n° 35252/08.

¹¹³ En précisant les motifs d'autorisation d'une interception, la procédure d'octroi de cette autorisation, les circonstances d'interception d'un individu, les procédures à suivre pour la sélection/examen et utilisation des éléments interceptés, les précautions pour la communication, la durée de l'interception et de la conservation de ces données.

¹¹⁴ Les procédures et modalités de supervision par une autorité indépendante et les procédures de contrôle indépendant a posteriori du respect des garanties.

recours généralisé à de tels systèmes serait vraisemblablement considéré comme attentatoire aux droits fondamentaux par les juridictions européennes¹¹⁵.

2. Liberté d'expression, de croyance et d'assemblée et le chilling effect

-35. Utilisées pour surveiller les espaces accessibles au public, les technologies de surveillance physiognomoniques peuvent parallèlement entraver l'exercice de la liberté d'expression, de croyance ou d'assemblée. Dès lors que ces libertés sont conventionnellement consacrées, la menace a fait l'objet de plusieurs mises en garde de la part des Nations Unies¹¹⁶. Le fait d'être reconnu ou catégorisé dans les espaces accessibles au public expose potentiellement les croyances, appartenances ou oppositions des individus. Rappelons que l'une des fonctionnalités de la reconnaissance faciale est l'identification et le traçage de personnes d'intérêt, susceptibles de troubler la tranquillité publique. Les opposants politiques peuvent, à ce titre, figurer sur les listes. Il s'agit d'une pratique répandue à l'échelon global, l'histoire récente l'illustrant tristement. Mentionnons à ce titre le recours à cette technologie en Afghanistan contre les citoyens ayant collaboré avec les anciennes puissances occupantes¹¹⁷, en Birmanie contre les Rohingyas¹¹⁸, à Hong Kong pour réprimer la révolution des parapluies¹¹⁹, en Inde contre les populations musulmanes¹²⁰, en Russie¹²¹ contre les opposants au régime ou à l'encontre des populations ouïgoures en Chine.

¹¹⁵ C. LEQUESNE ROTH, « De la fin de l'anonymat : reconnaissance faciale et droit à la vie privée », *Dalloz IP/IT*, Juin 2021, pp. 308-313.

¹¹⁶ OHCHR *Rights to freedom of peaceful assembly and of association - Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association*, 17 May 2019, A/HRC/41/41; OHCHR, *Surveillance and human rights - Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, 28 May 2019, A/HRC/41/35. UN Human Rights Commissioner, *Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests*, Report of the United Nations High Commissioner for Human Rights, 24 June 2020, A/HRC/44/24; International Network of Civil Liberties Organizations (INCLIO), *Facial Recognition Tech Stories and Rights Harms from around the World*, January 2021, pp. 5-8; pp 13-17.

¹¹⁷ HUMAN RIGHTS WATCH, *Afghanistan : Les systèmes de données biométriques mettent en danger de nombreux Afghans*, 30 mars 2022, [en ligne](#).

¹¹⁸ R. CHANDRAN, « They tried to erase us': Rohingya IDs deny citizenship », *Thomson Reuters report*, 18 novembre 2022, [en ligne](#).

¹¹⁹ « In Hong Kong protests, faces become weapons, *New York Times*, 26 juillet 2019, [en ligne](#).

¹²⁰ S. SANTOSHINI, « Indian police use facial recognition to persecute Muslims and other marginalized communities », *Coda*, 11 octobre 2022, [en ligne](#); E. TRUJILLO, « En Inde, la reconnaissance faciale utilisée pour surveiller les manifestants », *BFMTV*, 30 décembre 2019, [en ligne](#).

¹²¹ HUMAN RIGHTS WATCH, *Russia uses facial recognition to hunt down draft evaders*, 27 août 2021, [en ligne](#).

L'identification de catégories d'individus, sans même établir leur identité civile, peut s'avérer tout aussi menaçante. Le régime iranien recourt ainsi à la vidéosurveillance intelligente pour repérer et sanctionner les femmes qui ne portent pas le hijab¹²². De la même manière, les autorités serbes l'utilisent pour repérer les populations Roms¹²³. Demain ces technologies pourraient, comme elles en font la promesse¹²⁴, être mises au service de la pseudo-identification des personnes homosexuelles ou des personnes adeptes d'un culte en se fondant sur leur tenue vestimentaire.

-36. Il est intéressant de relever que l'atteinte opère de deux manières. Dans les cas évoqués, les technologies physiognomoniques exercent une **atteinte directe** : l'identification technologique à une appartenance ou de l'organisation d'un rassemblement emportent une immédiate sanction. Dans nos régimes démocratiques, la menace s'exerce également, de manière indirecte, au travers de ce que l'on désigne communément comme le « **chilling effect** »¹²⁵. Celui-ci décrit communément le fait, pour une personne redoutant une sanction juridique ou une atteinte à son intimité, de s'autocensurer ou de ne pas exercer un droit qui lui est légitimement accordé. Pour paraphraser la CJUE, la technologie exerce dans cette seconde hypothèse, « un effet stigmatisant entraînant à son tour un effet dissuasif » des « opposants politiques » à rejoindre ou à soutenir des actions associatives¹²⁶. Certains auteurs ajoutent qu'elle opère dans la positive un effet de « conformité » ou « d'obéissance anticipée » au mépris des croyances individuelles¹²⁷. L'identification de ce risque induit est corroborée par

¹²² "Iran Says Face Recognition Will ID Women Breaking Hijab Laws", *Wired*, 18 janvier 2023, [en ligne](#).

¹²³ AMNESTY INTERNATIONAL, *Serbia: Social Card law could harm marginalized members of society – legal opinion*, November 28, 2022, [en ligne](#).

¹²⁴ Y. WANG & M. KOSINSKI, "Deep Neural Networks Are More Accurate Than Humans at Detecting Sexual Orientation From Facial Images", 114 *J. PERSONALITY, & SOC. PSYCH.* 246 (2018), cité par L. STARK and J. HUTSON, "Physiognomic Artificial Intelligence", *op cit*.

¹²⁵ Notons qu'en matière doctrinale, le chilling effect a principalement été conceptualisé par la doctrine anglophone. L'article « fondateur » est celui de Frederick SCHAUER, "Fear, Risk, and the First Amendment: Unraveling, the "Chilling Effect"", 58 *B.U. L. REV.* 685 (1978) cité par OPEN SOCIETY, *The Concept of Chilling Effect*, 2021, [en ligne](#). On trouve la création de cette notion dans l'arrêt de la CEDH *Donnelly and others v. UK*, 5 Avril 1973. Nous invitons la/le lectrice/lecteur intéressé(e) à consulter la note de bas de page n°6 de J. W. PENNEY, « Understanding chilling effects », *Minnesota Law review*, n°16 p. 1451 et s., en [ligne](#), qui fait état d'une bibliographie importante.

¹²⁶ Case C-78/18, *Commission v. Hungary*, EU:C:2020:476. Les commentateurs de cet arrêt soulignent que « les mesures contestées ne sont pas des exemples singuliers de mauvaise loi, mais plutôt représentatives d'un schéma plus large qui a vu des "autocrates légalistes" utiliser délibérément une réglementation juridique visant à réduire ou à supprimer tout degré de dissidence ou de désaccord dans l'espace public et politique ». P. BARD, J. GROGAN and L. PECH, "The Democratic and Pluralist Society and its Enemies: The Court of Justice to the Rescue of Civil Society in the Member States", *Reconnect blog*, 23 June 2020.

¹²⁷ M. BUCHI, N. FESTIC et M. LATZER, "The Chilling Effects of Digital Dataveillance: A Theoretical Model and an Empirical Research Agenda", *Big Data society*, Vol. 9 issue 1, 2022 pp.14, spec. p.4.

les enquêtes sociologiques. Deux phénomènes ont été observés : le comportement des individus évolue en présence de caméras¹²⁸ et les lieux équipés de caméras sont tendanciellement désertés¹²⁹. À l'inverse, le droit d'aller et venir librement a pour condition celui de s'assurer que les individus puissent le réaliser anonymement¹³⁰. Plusieurs autorités, à l'instar du Contrôleur européen des données¹³¹, de la Commission nationale consultative des droits de l'homme (CNCDH)¹³² ou de l'agence européenne des droits fondamentaux (FRA)¹³³ ont ainsi, d'ores et déjà, alerté sur ce risque d'entrave technologique. En tout état de cause tous insistent sur le fait que les usages présentent ***un risque de surveillance de masse*** qui constituerait une atteinte majeure aux libertés. Pour être conformes aux impératifs démocratiques, les régimes d'encadrement devront nécessairement prévoir des usages très restreints, déclinés ***de l'interdiction ferme au régime de redevabilité renforcée***. Avant d'envisager ces mesures, examinons le régime en vigueur.

¹²⁸ B. KNIJNENBURG, X. PAGE, P. WISNIEWSKI, H. RICHTER-LIPFORD, N. PROFERES et J. ROMANO, *Modern Socio-Technical Perspectives on Privacy*, Springer, 2022, pp. 459, spéc. p. 245 « In the public DOMAIN, security cameras cause people to change their behavior when they perceive they are being watched. In public, CCTVs can result in less anti-social behavior and reduce crime. Yet, as smart cameras move into more private spaces, constantly being watched may have a chilling effect on behavior, particularly for those who lack control over the cameras ».

¹²⁹ F. CASTAGNINO, « Rendre « intelligentes » les caméras : déplacement du travail des opérateurs de vidéosurveillance et redéfinition du soupçon », op cit.

¹³⁰ P. KELLY, *Facial recognition technology and the growing power of artificial intelligence - Report of the Standing Committee on Access to Information, Privacy and Ethics pour le compte du parlement canadien*, pp. 84 spéc. p. 32, sur l'audition de Mme C. Khoo, [en ligne](#).

¹³¹ EDPS, Avis 4/2015, *Data ethics*, p. 8, "Drones, or semi-autonomous aircraft, currently serve mainly military purposes, but are increasingly used for purposes of surveillance, mapping, transportation, logistics and public security, such as containing wildfires²⁵. Photographs, videos and other personal data collected by drones can be exchanged over telecommunications networks. Their use risks serious interference with privacy and a chilling effect on freedom of expression".

¹³² CNCDH, *Avis sur la proposition de loi relative à la sécurité globale*, Assemblée plénière du 26 novembre 2020, JORF n° 0290 du 1er décembre 2020, texte n° 83.

¹³³ FRA, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 27 Novembre 2019, [en ligne](#).



III. Les lacunes des régimes applicables aux technologies physiognomoniques

-38. Les régimes applicables aux technologies physiognomoniques relèvent à ce jour de dispositions disparates. Dès lors qu'elles engagent le traitement de données biométriques, elles relèvent notamment de la législation nationale et européenne en vigueur en matière de protection des données¹³⁴. Dans les débats législatifs en cours, deux textes sont en passe de compléter cet arsenal légal : à l'échelon national, la loi d'expérimentation pour les JO 2024, dont l'article 7 prévoit des mesures d'encadrement applicables à la vidéosurveillance intelligente ; à l'échelon européen, l'AIA qui trace des lignes concernant l'usage de la reconnaissance faciale et comportementale. L'étude de l'ensemble de ces dispositions s'articulera en trois temps.

¹³⁴ Le règlement général sur la protection des données (UE) 2016/679 du 27 avril 2016 (RGPD) et la loi Informatique et libertés n° 78-17 du 6 janvier 1978 d'une part, la directive police justice (UE) 2016/680 du 27 avril 2016 et le code de la sécurité intérieure de l'autre, constituent les principaux textes de référence.

Premièrement, nous nous efforcerons de démontrer qu'en l'absence de dispositions idoines, les déploiements – expérimentaux ou pérennes- de ces technologies ne bénéficient pas de fondement légal adapté (A). De même, les garanties ne couvrent pas entièrement les risques identifiés : nous l'établirons par l'examen du droit en vigueur (B). Enfin, nous soutiendrons que les lacunes tiennent encore à la méthode : l'expérimentation, fortement encouragée et privilégiée, est pour l'heure exclusivement conçue sous l'angle technique, bien souvent au mépris des processus démocratiques (C).

A. L'absence de fondements légaux adaptés

-39. À ce jour, l'existence de base légale idoine fait obstacle au déploiement des technologies physiognomoniques à des fins d'identification dans les espaces accessibles au public. Le Conseil Constitutionnel l'a rappelé à l'occasion de l'examen de la Loi relative à la responsabilité pénale et à la sécurité intérieure : les dispositions de l'article L. 242-4 du code de la sécurité intérieure, interdisant les traitements automatisés de reconnaissance faciale par les dispositifs aéroportés, « ne sauraient, sans méconnaître le droit au respect de la vie privée, être interprétées comme autorisant les services compétents à procéder à l'analyse des images au moyen d'autres systèmes automatisés de reconnaissance faciale qui ne seraient pas placés sur ces dispositifs aéroportés »¹³⁵. En d'autres termes, les forces de l'ordre ne sont pas autorisées à recourir à ces systèmes en l'absence de dispositions législatives les y autorisant. La CNIL rappelle, dans le même sens, que le seul intérêt légitime - qui fonde le déploiement de la vidéoprotection - ne constitue pas davantage une base légale suffisante si la « mission d'intérêt public » dans lequel il s'inscrit n'est pas « prévue et encadrée » dans le droit de l'Union européenne ou le droit français¹³⁶.

-40. Cette position résulte en outre de l'inadaptation des bases légales existantes. Conformément à la distinction de principe opérée par la Cour de cassation¹³⁷, lorsque ces technologies sont mobilisées au service de la prévention, leur déploiement relève du régime de police administrative et sont soumises au RGPD ; dès lors qu'elles s'inscrivent dans le cadre d'une procédure pénale - et conduisent à une arrestation – elles relèvent du régime de police

¹³⁵ Cons. Const. Décision n° 2021-834 DC du 20 janvier 2022.

¹³⁶ CNIL, *Caméras dites « intelligentes » ou « augmentées » dans les espaces publics*, précédemment cité, p.12.

¹³⁷ Cass. Crim. 4 juin 1991, no 91-81.682.

judiciaire et de la directive police justice. Tandis que le RGPD interdit, par principe, les traitements de données biométriques (article 9), la directive police justice les limite à la stricte nécessité (article 10). Les deux textes prévoient toutefois des exemptions permettant, en théorie, le déploiement de ces systèmes. Néanmoins, ces fondements sont inadaptés au déploiement des technologies physiognomoniques dans les espaces accessibles au public, en étudiant, successivement, les fondements communs aux deux régimes (1), puis ceux spécifiques à la police administrative (2).

1. Les fondements communs aux régimes administratifs et judiciaire

-41. Le RGPD et la directive police justice prévoient trois exceptions communes permettant, théoriquement, le déploiement de systèmes d'IA physiognomonique : la sauvegarde des intérêts vitaux d'une personne concernée ou d'autres personnes physiques (a), le traitement de données manifestement rendues publiques (b), ou l'existence d'une loi, traduisant un intérêt légitime dans le RGPD (c). Seul ce dernier fondement semble potentiellement valable. Toutefois, à ce jour, seul un projet de loi autorisant un déploiement expérimental y correspond.

a. La sauvegarde des intérêts vitaux

-42. La direction justice et le RGPD mentionnent tous deux la « protection de l'intérêt vital de la personne concernée ou d'une autre personne physique »¹³⁸ comme autre exception à l'interdiction des traitements de données biométriques. La pertinence de cette base juridique a pu être interrogée dans le contexte pandémique. Le considérant 46 du RGPD précise en effet que l'exemption peut concerner le traitement nécessaire « à la surveillance des épidémies et de leur propagation ». Certaines villes ont expérimenté des systèmes de reconnaissance physiognomonique pour assurer la sécurité sanitaire. À Cannes, un système repérant les personnes ne portant pas le masque fut mis en place au titre de la lutte contre la propagation du virus¹³⁹. Une expérience similaire a été conduite dans le métro parisien¹⁴⁰. Dans un avis circonstancié, la CNIL avait toutefois jugé que le système, même « limité au cadre de l'état d'urgence sanitaire », présentait « le risque réel de généraliser un sentiment de surveillance

¹³⁸ Article 9§2(c) du RGPD et article 10 (b) de la directive police justice.

¹³⁹ A Cannes, des tests pour détecter automatiquement par caméras le port du masque, *Le Monde*, 28 avril 2020.

¹⁴⁰ La RATP va tester des caméras « intelligentes » pour mesurer le taux de port du masque dans la station Châtelet, *Le Monde*, 7 mai 2021. Ces expérimentations ont, toutefois, été suspendues après la position de la CNIL.

chez les citoyens, de créer un phénomène d'accoutumance et de banalisation de technologies intrusives et, en définitive, d'engendrer une surveillance accrue »¹⁴¹. Le projet fut aussi abandonné.

-43. Néanmoins, selon le Comité européen de protection des données (CEPD)¹⁴² – et conformément à l'article 46 du RGPD – cette exception n'est mobilisable que si la personne concernée est incapable (en droit ou en pratique) de donner son consentement au traitement, ce qui implique que la personne concernée manque de capacité. En tant que telle, cette base juridique semble réservée aux seules situations d'urgence. Cette exemption ne constitue donc pas une base juridique générale pour le déploiement des systèmes physiognomoniques dans les espaces accessibles publics. Ainsi après avoir vu l'(in)application des différents fondements proposés par le RGPD, subsiste la question du traitement des données volontairement publiées par la personne concernée.

b. Les données manifestement rendues publiques

-44. La directive justice et le RGPD autorisent également le traitement des données biométriques lorsque celles-ci ont été « manifestement rendues publiques par la personne concernée »¹⁴³. La signification de cette disposition a été débattue par des autorités européennes de protection des données¹⁴⁴. Dans ses lignes directrices, cependant, le CEPD exclut cette disposition comme base juridique pour le déploiement de systèmes de reconnaissance faciale en temps réel dans les espaces accessibles au public. Il rappelle que « le simple fait d'entrer dans le champ de la caméra n'implique pas que la personne concernée ait l'intention de rendre publiques des catégories particulières de données la concernant »¹⁴⁵. Le Comité en conclut que les responsables de traitements de données biométriques ne peuvent

¹⁴¹ Délibération n° 2020-136 du 17 décembre 2020 portant avis sur un projet de décret relatif au recours à la vidéo intelligente pour mesurer le taux de port de masque dans les transports.

¹⁴² Article 9 (2) (c) « peut – en théorie et exceptionnellement – être utilisé, mais les responsables du traitement doivent justifier de la nécessité absolue de sauvegarder les intérêts vitaux d'une personne et de démontrer (...) l'impossibilité pour la personne concernée, ou de son responsable légal, de donner son consentement ». De plus, le responsable du traitement n'est pas autorisé à utiliser le système pour d'autres finalités. CEPD, *Guidelines 3/2019 on processing of personal data through video devices* (2020), Version 2.0, January 29, §69.

¹⁴³ Article 9§2(e) RGPD and 10 (c) directive justice.

¹⁴⁴ Dove E.S., Chen J., *What does it mean for a data subject to make their personal data “manifestly public”? An analysis of GDPR Article 9(2)(e)*, University of Edinburgh School of Law Working Paper, No 2020/18.

¹⁴⁵ EDPD, *Guidelines 3/2019 on processing of personal data through video devices* (2020), *op. cit.* §70.

se fonder sur l'article 9, paragraphe 2, point e) dans le cadre de la vidéosurveillance intelligente.

-45. La question de savoir si cette exemption pouvait fonder les traitements de données biométriques s'est toutefois posée à l'occasion de l'affaire Clearview. Cette société a construit la plus grande base de données biométriques existante à partir de données récupérées sur les médias sociaux. Plusieurs autorités de protection des données canadiennes et européennes furent saisies par des associations de défense des droits¹⁴⁶. L'affaire offrit à la CNIL l'occasion de se prononcer sur la disposition. Elle considéra que « le caractère 'publiquement accessible' d'une donnée n'influe pas sur la qualification de donnée à caractère personnel et qu'il n'existe aucune autorisation générale permettant de réutiliser et de traiter de nouveau des données à caractère personnel publiquement disponibles, en particulier à l'insu des personnes concernées ». Aussi, la société ne pouvait se prévaloir d'un quelconque intérêt légitime sur l'exploitation des données personnelles volontairement divulguées par les personnes concernées, ces dernières ne disposant d'aucune attente raisonnable d'un tel traitement¹⁴⁷.

Il en résulte que l'exemption due aux données « manifestement rendues publiques par la personne concernée » ne constitue pas davantage un fondement légal valable au déploiement d'IA physiognomoniques.

c. Le droit de l'Union ou du droit d'un État membre

-46. L'exemption légale constitue le troisième fondement au déploiement d'un traitement biométrique commun au RGPD et à la directive police justice¹⁴⁸. Notons plus largement, au regard des précédents développements, que l'existence d'un fondement légal est de surcroît une exigence conventionnelle dès lors que les systèmes développés sont susceptibles de porter atteinte à la vie privée. Le recours à la reconnaissance faciale par la police galloise pour la sécurisation d'événements sportifs et culturels a ainsi été sanctionné sur le fondement de

¹⁴⁶ Sur l'histoire et les ramifications de ce contentieux, voy. C. LEQUESNE ROTH, « Mise en demeure de Clearview AI par la CNIL : les jalons d'un combat pour le droit à l'anonymat », *Dalloz IP/IT*, avril 2022.

¹⁴⁷ CNIL Délibération de la formation restreinte n° SAN-2022-019 du 17 octobre 2022 concernant la société CLEARVIEW AI.

¹⁴⁸ Art. 10 §a., là où l'art. 9 §2 g) RGDP renvoie à des « motifs d'intérêt public important »

l'article 8 de la Convention européenne des droits de l'homme : à défaut de disposition légale, « le cadre juridique en place » a été jugé « insuffisant »¹⁴⁹.

-47. À ce jour, aucun État de l'Union européenne n'a adopté de législation nationale relative aux traitements physiognomoniques. Différents projets de loi ont été proposés en matière de reconnaissance faciale, mais aucun d'entre eux n'a été adopté¹⁵⁰. Si l'idée d'autoriser le recours à cette technologie pour les Jeux olympiques 2024 a été, un temps, envisagée en France¹⁵¹, elle a pour l'heure été écartée. Le projet de loi relative au JO prévoit néanmoins d'autoriser, à titre expérimental pour la période 2023-2025, le recours à la vidéosurveillance intelligente. Notons que dans l'état actuel de sa rédaction, la loi est ambiguë : si elle exclut expressément le recours aux traitements biométriques¹⁵², elle n'en prévoit pas moins implicitement la légalisation de l'IA comportementale nécessaire à la prévention d'infractions¹⁵³. Or, rappelons que les données comportementales constituent des données biométriques¹⁵⁴. Cette loi n'en constituerait pas moins, à date, le fondement légal le plus solide au déploiement de certaines IA physiognomoniques dans les espaces accessibles au public.

-48. Si une loi venait à pérenniser ces usages, son cadre reste à définir. La législation européenne ne donne aucune indication sur la manière dont l'intérêt ou la nécessité publics peuvent être évalués¹⁵⁵, laissant la voie ouverte à l'interprétation nationale. Cela soulève un double problème : d'une part, la protection accordée est susceptible de varier considérablement d'un pays à l'autre ; de l'autre, l'intérêt public étant large, certaines juridictions peuvent poursuivre des projets risqués.

¹⁴⁹ [2020] EWCA Civ 1058 §90, §91.

¹⁵⁰ En France et en République tchèque. Voir notamment *New Surveillance Technologies in Public Spaces*, op cit p.65.

¹⁵¹ Voir *Office parlementaire d'évaluation des choix scientifiques et technologiques de l'Assemblée Nationale*, « Reconnaissance faciale », *Briefing Science et technologie*, No. 14, Juillet 2019.

¹⁵² Art. 7-III.

¹⁵³ Art. 7 I.

¹⁵⁴ Voir *supra* n°7.

¹⁵⁵ Le Considérant 45 du RGPD ne prévoit que l'implémentation de mesures de protection.

-49. Notons qu'en dépit de la publicité qui entoure l'AIA, et de l'importance accordée à la reconnaissance faciale dans les débats qui l'entourent, cette proposition de règlement n'apporte pas tous les éléments d'éclaircissement espérés.

En effet, si l'article 5 interdit, par principe, « l'utilisation de systèmes d'identification biométrique à distance » en temps réel » dans des espaces accessibles au public par les autorités répressives ou en leur nom à des fins répressives », les exceptions sont nombreuses. D'une part, l'article 5(d) prévoit que le recours à ces systèmes est admis pour :

- (i) *la recherche ciblée de victimes potentielles spécifiques de la criminalité ;*
- (ii) *la prévention d'une menace spécifique, substantielle et imminente pour la vie ou la sécurité physique des personnes physiques ou la prévention d'une attaque terroriste;*
- (iii) *la détection, la localisation, l'identification ou les poursuites à l'encontre de l'auteur ou du suspect d'une infraction pénale visée à l'article 2, paragraphe 2, de la décision-cadre 2002/584/JAI du Conseil 62 et punissable dans l'État membre concerné d'une peine ou d'une mesure de sûreté privatives de liberté d'une durée maximale d'au moins trois ans, déterminées par le droit de cet État membre.*

D'autre part, au titre de l'article 5(4), un État membre pourrait décider d'autoriser totalement ou partiellement l'utilisation de ces systèmes dans les espaces accessibles au public à des fins répressives. Dans ces hypothèses, l'AIA constituerait une base légale valable. Toutefois, au regard de ce qui précède, et en tout état de cause dans la seconde hypothèse, le législateur devrait préciser les conditions de déploiement des systèmes et les garanties qui l'entourent.

-50. Notons enfin que des dispositions spécifiques autorisent le déploiement de traitements biométriques aux frontières. L'Union européenne et ses États membres peuvent collecter de nombreuses données personnelles – y compris biométriques – dans le cadre du Programme Schengen Information System (SIS)¹⁵⁶. Les articles 32 et 33 du Règlement correspondant prévoient les modalités de collecte de ces données et leurs conditions d'utilisation. Elles peuvent être mobilisées pour identifier un citoyen extraeuropéen aux frontières. Le site

¹⁵⁶ Encadré par le Règlement 2018/661 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.

Internet du SIS informe que le système n'utilise pas encore la reconnaissance faciale, tout en précisant que les États membres sont libres d'y recourir¹⁵⁷ ; la reconnaissance émotionnelle et comportementale a sur ces fondements déjà été déployée à titre expérimental¹⁵⁸. Toutefois, ces traitements européens sont propres à la sécurité des frontières dérogeant au droit national des États membres de l'Union européenne, spécifiquement le droit administratif en France.

2. Les fondements propres au régime administratif

-51. D'autres fondements sont susceptibles d'être mobilisés sous l'empire du RGPD. La CNIL a notamment eu l'occasion de les invoquer dans son rapport relatif à la vidéosurveillance intelligente. Notons que ces fondements ne semblent pas davantage adaptés au déploiement des IA physiognomoniques dans les espaces accessibles au public. Il s'agit du consentement d'une part (a), de l'exécution d'un contrat ou d'une mission de l'autre (b).

a. Le consentement

-52. À l'exception de certains traitements relevant de l'authentification¹⁵⁹, le fondement du consentement apparaît mal adapté au déploiement des technologies de surveillance physiognomoniques dans les espaces accessibles au public. À cela, deux raisons majeures. La première est d'ordre pratique et matérielle : recueillir le consentement de chaque individu dans le cadre de la surveillance d'une foule relève de la gageure. De surcroît, le refus d'une partie du public concerné rendrait impossible la captation.

¹⁵⁷ Commission européenne, *What is SIS and how does it work*, [en ligne](#), "SIS does not yet use photograph and facial image recognition technology. The Commission must provide a report on the availability, readiness and reliability of such technology before this can be put in place. The European Parliament will be consulted on the report. Once this technology is put in place in SIS, countries will be able to use these tools at regular border crossing points. After that, the Commission may adopt delegated acts determining other circumstances in which photographs and facial images may be used to identify persons".

¹⁵⁸ Voir *supra* n°14.

¹⁵⁹ L'authentification par reconnaissance faciale offre un environnement de contrôle plus propice au recueillement du consentement, ce qui en fait une base légale pour – notamment et non exclusivement – des usages commerciaux. C'est sur ce fondement que se déploie aujourd'hui de nombreux usages de la technologie à l'instar du déverrouillage des smartphones, des systèmes de paiement ou de l'authentification en ligne sur certaines plateformes (publique ou privée). Voir aussi, *infra*, le système Alicem.

Le second tient à la légitimité du consentement. Pour être valable, un consentement doit être libre et éclairé, à savoir « délivré en dehors de tout contexte de domination, d'aliénation ou de discrimination propres à certaines sphères d'activités humaines [causant] un trop grand déséquilibre »¹⁶⁰. En matière de reconnaissance faciale, celui-ci a pu être caractérisé dans le cadre du déploiement de la technologie dans un lycée. L'expérimentation azurée a en effet été sanctionnée par le juge administratif au motif de la « relation d'autorité » existante entre la direction de l'établissement et les élèves qui entravait la liberté de choix de ces derniers¹⁶¹. Notons que le Conseil d'État, en dépit des réserves de la CNIL, s'est montré plus conciliant dans le contentieux Alicem¹⁶², où il était argué que les ressortissants étrangers destinataires de ce service se trouvaient « contraints » de fournir leurs données biométriques. La différence d'appréciation procède toutefois d'un double paramètre : d'une part, le service en question relevait de l'authentification et non de l'identification dans une foule ; de l'autre, il intégrait des moyens alternatifs garantissant, selon la Haute juridiction, une liberté de choix. Au regard de ces éléments, il apparaît peu probable que les conditions d'un choix « libre et éclairé » puissent être réunies dans le cadre du déploiement de technologie physiognomonique dans les espaces accessibles au public.

b. L'exécution d'un contrat

-53. Étrangement, la CNIL prévoit également la possibilité d'invoquer le fondement de l'exécution contractuelle¹⁶³. Elle pose à cet égard deux conditions : que le contrat soit conclu entre le responsable et la personne concernée ; elle mentionne ainsi l'exemple d'un contrat ayant pour objet la fourniture d'un service nécessitant le déploiement des caméras « augmentées » ; d'autre part, que le traitement automatisé de l'image des personnes par des caméras « augmentées » soit nécessaire à son exécution¹⁶⁴. Cette hypothèse se comprend dans le cadre de fonctions d'authentification. Elle semble toutefois inopérante dans le cadre des usages d'une IA physiognomonique à des fins d'identification dans les espaces accessibles au public. En effet, outre la légalité contestable d'un contrat qui la mettrait en place pour

¹⁶⁰ C. LAZARO, D. LE METAYER, *Le consentement au traitement des données personnelles : une perspective comparative sur l'autonomie du sujet*, *Revue juridique Thémis de l'Université de Montréal*, vol. 48, 2014, p. 766.

¹⁶¹ [TA Marseille 27.02.2020](#).

¹⁶² CE, 10ème - 9ème chambres réunies, 04/11/2020, 432656, *Inédit au recueil Lebon*.

¹⁶³ CNIL, *Caméras dites « intelligentes » ou « augmentées » dans les espaces publics*, précédemment cité, p. 12.

¹⁶⁴ *Ibidem*.

toutes les raisons déjà mentionnées, le consentement éclairé de la personne concernée semble en ces circonstances difficile à fournir sans qu'un lien de « soumission » quelconque n'en vicie la validité. Le contrat n'apparaît donc pas comme un fondement réellement satisfaisant pour les traitements d'IA physiognomoniques. Ainsi une loi circonstanciée, assortie de nombreuses garanties, apparaît comme la seule base juridique mobilisable pour fonder un tel déploiement. Néanmoins, ces garanties ne sont pas absolues et comprennent de nombreuses lacunes.

B. Les garanties incertaines du régime en vigueur

-54. Le régime de redevabilité en vigueur s'articule autour de cinq catégories de garanties dont nous étudierons successivement les obligations : les garanties dues au titre de la protection des données (1), celles incombant au responsable de traitement (2), les garanties techniques (3), les garanties humaines (4) et les droits des personnes concernées (5). Or, les systèmes physiognomoniques s'opposent, par leur nature même ou leurs usages, à l'établissement de certaines de ces garanties.

1. Les garanties dues au titre de la protection des données

-55. Les textes européens relatifs à la protection des données personnelles applicables aux technologies physiognomoniques convergent autour de six grands principes à appliquer pour qu'un traitement offre des garanties suffisantes aux droits et libertés : le traitement doit être légal (a), ses finalités définies (b); il doit encore être proportionnel (c), minimiser la collecte des données (d), en assurer l'exactitude (e) et offrir des garanties en termes de conservation (f). Toutefois, il reste difficile de s'y conformer pour le déploiement d'IA physiognomoniques.

a. Légalité et nécessité du traitement

-56. La première exigence tient dans l'existence d'un fondement légal. Or, celui-ci demeure fragile et mérite d'être consolidé par le législateur.

-57. Le droit européen établit traditionnellement une interaction entre la légalité et la nécessité d'un traitement. En effet, la légalité d'un traitement s'immisçant dans les droits et libertés des citoyens ne fonde pas de façon autonome l'emploi de nouvelles techniques intrusives, il faut aussi que cette dérogation réponde à un besoin impérieux¹⁶⁵. Cette dernière condition s'exprime lors de l'examen de la proportionnalité.

b. Définition des finalités du traitement

-58. Cette seconde condition dans les obligations de conformité du responsable du traitement le contraint à devoir expliciter chaque utilisation de données personnelles pour l'information des personnes concernées¹⁶⁶, c'est-à-dire préciser quelle(s) donnée(s) personnelle(s) est/sont collectée(s) pour quelle utilisation. Le respect du principe de finalité prohibe la réutilisation non explicite de données. Ainsi, la collecte de données biométriques dont la finalité est précisée doit respecter la destination prédéfinie, et un traitement secondaire, potentiellement basé sur un second fondement légal, ne pourra pas être opéré. En d'autres termes, la définition des finalités du traitement de données biométriques implique que le responsable du traitement définisse chaque finalité de chaque traitement pour chaque type de données collectées. Cette précision complexifiera, en pratique, le travail du département juridique qui doit parallèlement faire œuvre de pédagogie à des fins informatives¹⁶⁷. La CNIL est particulièrement attentive aux informations fournies dont le défaut pourrait en outre être invoqué lors d'un recours.

c. Proportionnalité des traitements

-59. Selon le RGPD, le traitement des données biométriques peut être autorisé par le droit de l'Union ou des États membres, mais « doit être proportionné à l'objectif poursuivi » (article 9.2.g). La directive police justice ne soumet pas explicitement le traitement des données biométriques à la proportionnalité de l'usage, mais le laisse entendre dans le considérant 26

¹⁶⁵ Cons. Const. Décision n° 2021-834 DC du 20 janvier 2022.

¹⁶⁶ Voir *infra* n°69.

¹⁶⁷ Voir *infra* n°68.

: « tout traitement de données à caractère personnel (...) peut être effectué à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière (...), pour autant qu'il soit prévu par la loi et constitue une mesure nécessaire et proportionnée dans une société démocratique ». Pour évaluer la proportionnalité d'un système, la CJUE a établi un test de trois étapes. La Cour évalue (1) l'efficacité (2) la nécessité (et la subsidiarité) et (3) la proportionnalité du traitement¹⁶⁸.

-60. Comme nous l'avons établi au sujet de la reconnaissance faciale¹⁶⁹, les juridictions administratives et les autorités nationales de protection des données considèrent comme disproportionné tout usage lorsqu'une alternative moins attentatoire aux libertés peut lui être substituée. Le recours à des systèmes d'identification biométrique dans les écoles a, pour ce motif, été jugé disproportionné par le Datainspektionen suédois¹⁷⁰ et le tribunal administratif de Marseille¹⁷¹. De même, la CNIL considère que l'usage de ces technologies doit être exclu dans les cantines, des moyens alternatifs de surveillance étant suffisants¹⁷². L'ayant admis, a contrario, pour réguler le trafic aérien et assurer la sécurité des passagers à l'embarquement¹⁷³, on observe que la CNIL opère un contrôle de proportionnalité en statuant de manière casuistique, à l'aune des usages et des environnements. Cette approche se retrouve également dans sa note relative aux caméras intelligentes.

-61. Notons toutefois que le test de proportionnalité n'est pas pleinement satisfaisant, au regard de la nature particulièrement intrusive des traitements physiognomoniques. Ceux-ci peinent en effet à offrir par nature des garanties solides sur les différents volets examinés, comme nous le verrons pour la minimisation des données ou les mesures à adopter en cas de violation de données.

¹⁶⁸ CJUE, gde ch., 6 oct. 2020, aff. C-511/18, *La Quadrature du net*, rappelé par CJUE 2 mars 2021, aff. C-746/18, *H.K./Prokuratuur*

¹⁶⁹ *New Surveillance Technologies in Public Spaces*, op cit, p.66.

¹⁷⁰ DATAINSPEKTIONEN, *Lagändring krävs för att polisen ska kunna utföra testverksamhet av ansiktsverifiering på flygplats*, 16 December 2019.

¹⁷¹ TA Marseille, 27 February 2020, n°1901249. See above n°84.

¹⁷² CNIL, *Expérimentation de la reconnaissance faciale dans deux lycées : la CNIL précise sa position* 29 octobre 2019, <https://www.cnil.fr/fr/experimentation-de-la-reconnaissance-faciale-dans-deux-lycees-la-cnil-precise-sa-position>

¹⁷³ CNIL, *Reconnaissance faciale dans les aéroports: quels enjeux et quels grands principes à respecter ?*, 9 Octobre 2020.

d. Minimisation des données

-62. En dépit du principe de nécessité, la mise en œuvre d'un traitement ne justifie pas une collecte de toutes les données. L'article 5(c) du RGPD prévoit que seules les données strictement nécessaires à la réalisation du traitement doivent être recueillies. C'est le principe de minimisation des données, auquel est également soumis le responsable de traitements.

-63. En réalité, le respect de cette obligation est particulièrement délicat dans le cadre du déploiement des IA physiognomoniques. Comme nous l'avons vu, les captations sont rarement ciblées : que ce soit pour reconnaître des individus ou des catégories d'individus, le système scanne le plus souvent l'ensemble de la foule. De surcroît, les solutions d'anonymisation, bien qu'existantes, ne peuvent garantir un parfait anonymat ne serait-ce que par le jeu des recoupements des bases de données¹⁷⁴. Il en résulte que le déploiement de ces systèmes soulève d'importantes difficultés au regard du principe de minimisation.

e. Exactitude des données

-64. L'article 5(d) du RGPD impose que les données traitées soient « exactes », c'est-à-dire qu'elles reflètent une réalité objective évitant une qualification erronée de la personne concernée. Cette obligation apparaît d'autant plus essentielle que ces systèmes ont vocation à orienter le travail des agents sur le terrain.

-65. Pourtant, ici encore la mise en conformité des IA physiognomoniques avec le droit en vigueur apparaît problématique. Cela tient tant aux jeux de données d'entraînement – qui permettent d'établir les gabarits (catégoriels ou individuels) –, qu'aux données captées, sur la base desquelles reposent les contrôles. Outre la nature hautement contestable de certaines catégorisations évoquées (identification de « profils » de criminels, identification de l'orientation sexuelle ou de certains comportements « significatifs »¹⁷⁵), la qualité même des

¹⁷⁴ Séminaire de la DINUM, 24 février 2023.

¹⁷⁵ Voir *supra* n°12.

données est en cause. Comme l'ont établi les travaux de C. GARVIE, l'acquisition de données de qualité¹⁷⁶ fait souvent défaut en amont comme en aval des systèmes. Cette situation est également préoccupante en France, au regard de la rareté des jeux d'entraînement et de la faiblesse des réseaux de caméras équipées¹⁷⁷. Les systèmes de reconnaissance ne sont pas, à ce jour, en mesure de fournir des résultats d'identification fiables : ils offrent davantage une pluralité de « candidats », charge à leurs utilisateurs d'identifier le suspect parmi ces derniers¹⁷⁸. Ainsi, les « faux positifs » sont encore nombreux. Le respect de l'exactitude des données dans le cadre du déploiement des IA physiognomoniques apparaît encore à ce jour une gageure.

f. Conservation des données

-66. Le droit des données personnelles impose un droit à l'oubli numérique : les faits et gestes des individus ne peuvent être définitivement gravés dans le silicium¹⁷⁹. Pour respecter cette obligation, le droit impose une conservation limitée des données personnelles. Une fois obsolètes, elles doivent être effacées.

-67. En matière de conservation des données, l'article 7 du projet de loi sur les JO interroge. Les données, collectées à des fins de surveillance lors des expérimentations, devront respecter la durée de conservation établie aux articles L.242-4 et L.252-5 du code de la sécurité intérieure¹⁸⁰. Cette obligation est expressément mentionnée. L'article 7 prévoit parallèlement que ces données peuvent être « converties » en données d'apprentissage, pour entraîner ultérieurement des systèmes d'IA. Or, s'agissant de cette seconde finalité, le projet de loi ne prévoit aucune limitation de conservation. Cette disposition apparaît donc contraire au RGPD

¹⁷⁶ C. GARVIE, "A Forensic Without the Science: Face Recognition in U.S. Criminal, Investigations, Center on Privacy & Technology" *Georgetown Law*, 2022 p. 18.

¹⁷⁷ M.-P. DAUBRESSE, A. de BELENT et J. DURAIN, *Sénat, Session 2021-2022, Rapport d'information n°627 fait au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale sur la reconnaissance faciale et ses risques au regard de la protection des libertés individuelles*, enregistré le 10 mai 2022, not. p. 63.

¹⁷⁸ C. GARVIE, "A Forensic Without the Science: Face Recognition in U.S. Criminal, Investigations, Center on Privacy & Technology", *op cit.*

¹⁷⁹ Voir le principe posé à l'article 5 (e) du RGPD, les données personnelles devant être « conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées ».

¹⁸⁰ Prévoyant respectivement une durée de 48 heures et de 1 mois.

dès lors que les données converties conservent leur qualité de données à caractère personnel. Cette pseudo-conversion des données, résultant d'un changement de finalité, ne permet pas de justifier à elle seule l'absence de garanties sur le terrain de la conservation.

2. Les garanties liées au responsable du traitement

-68. Outre les obligations de conformité internes à sa structure, le responsable du traitement est tenu à des obligations externes à l'égard de l'information préalable des personnes concernées. Il est à cet égard tenu à une obligation de transparence (a), corollaire de l'obligation d'information (b). Des obligations complémentaires lui incombent en cas de violation des données (c).

a. Obligations de transparence et d'information

-69. Le principe de transparence est établi à l'article 5 du RGPD comme le premier principe directeur relatif au traitement des données à caractère personnel. Le considérant 39 du RGPD précise qu'il exige que « toute information et communication relatives au traitement de ces données à caractère personnel soient aisément accessibles, faciles à comprendre, et formulées en des termes clairs et simples » aux personnes concernées. Son application est en pratique réalisée par les articles 12 à 14 du RGPD, qui énoncent les informations à fournir lorsque les données personnelles sont collectées directement ou indirectement auprès de la personne concernée. Le principe de transparence est de ce fait étroitement corrélé à l'obligation d'information à laquelle le responsable de traitement est soumis. Cependant, cette corrélation est source de confusions. À titre d'illustration, l'article 7 du projet sur les Jeux olympiques prévoit tout d'abord « une information générale du public sur l'emploi de traitements algorithmiques sur les images collectées », que l'on suppose relever du principe de transparence prévu par l'article 5 §1 (a) du RGPD. Le même article contraint par la suite à ce que l'autorité informe le public « par tout moyen approprié de l'emploi de traitements algorithmique au moyen de systèmes de vidéoprotection ». Cette publicité semble relever de l'obligation d'information prévue par l'article 14 du RGPD.

-70. L'obligation d'information varie en fonction de la base légale invoquée. Le fondement légal, sur lequel repose un traitement de données biométriques, présuppose que le traitement soit décrit de façon suffisamment claire dans la loi¹⁸¹. Il est inquiétant de noter que cette transparence « légale » justifie, dans la dernière version de l'article 32 de l'AIA, que le public ne bénéficie pas d'une explication sur les systèmes d'intelligence pour la prévention/détection d'infraction pénale (§1) ou pour la reconnaissance des émotions ou d'un système de catégorisation biométrique (§2). La reconnaissance des données physiognomoniques se trouve alors exclue de leur champ.

En revanche, dans l'hypothèse où le traitement a lieu dans un lieu privé recevant du public pour l'unique bénéfice d'un responsable de traitement de droit privé, le principe de transparence reprend toute sa vigueur. La personne concernée doit avoir une attente raisonnable à voir ses données biométriques être traitées par un algorithme et par conséquent doit en être informée¹⁸².

-71. Le principe de transparence exige que « toute information adressée au public ou à la personne concernée soit concise, aisément accessible et facile à comprendre, et formulée en des termes clairs et simples et, en outre, lorsqu'il y a lieu, illustrée à l'aide d'éléments visuels »¹⁸³. En termes pratiques, les lignes directrices sur la transparence du Groupe de travail de l'Article 29¹⁸⁴ fournissent des indications précieuses quant à la forme et au contenu des informations devant être fournies. Il préconise l'utilisation de visuels, de graphiques ou de logos. En effet, la compréhension d'un logo est accessible à l'ensemble des publics, y compris aux « personnes vulnérables »¹⁸⁵.

¹⁸¹ CEDH *Klass et autres c. Allemagne*. 6 septembre 1978.

¹⁸² Article 14 du RGPD.

¹⁸³ Considérant 58 du RGPD.

¹⁸⁴ *Lignes directrices sur la transparence au sens du règlement (UE) 2016/679, Adoptées le 29 novembre 2017, Version révisée et adoptée le 11 avril 2018, WP 260 rev. 01.*

¹⁸⁵ *Enfants, handicapés, personnes âgées.*



Figure 4 : exemple de logo de surveillance

Il ne semble toutefois pas constituer une solution optimale dans l'hypothèse où le système procède à divers traitements tels que la détection de menaces ou de comportements dangereux : en termes d'exhaustivité de l'information d'une part¹⁸⁶, de compréhension de la complexité des systèmes et de leurs enjeux de l'autre¹⁸⁷.

-72. Précisons enfin que l'obstacle le plus important à la mise en conformité à ces obligations tient aujourd'hui au recours à des sociétés privées, lesquelles refusent de communiquer les éléments techniques de leur système sur le fondement du secret des affaires. Tel fut le cas dans l'expérimentation niçoise de la reconnaissance faciale. La CNIL exigea, a posteriori, des évaluations techniques plus poussées qui n'étaient pas en la possession des autorités niçoises¹⁸⁸. L'affaire la plus retentissante sur ce point concerne « iBorderCtr », ce système déjà évoqué de détection des mensonges aux frontières. La demande de communication d'information introduite par le député européen Breyer auprès de l'Agence exécutive européenne pour la recherche n'ayant abouti, l'affaire fut portée devant la CJUE. La juridiction

¹⁸⁶ Comme le requièrent les articles 12 à 114 du RGPD. Le lieu d'hébergement des données doit par exemple, à ce titre, être renseigné.

¹⁸⁷ En témoignent de récentes études relatives à la compréhension des logos informatifs des traitements algorithmiques de données personnelles par des panels représentatifs. Voir, par exemple, les travaux de L. CRANOR, P. G. KELLEY, J. BRESEE, L. CRANOR, R. W. REEDER, A "Nutrition Label" for Privacy, Symposium On Usable Privacy and Security (SOUPS) 2009, July 15-17, 2009, ou encore Aleecia M. McDonald and Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, I/S: A Journal of Law and Policy for the Information Society 2008 Privacy Year in Review issue.

¹⁸⁸ DATATECHNOPOLICE, Réponse du 15 février 2019 de la CNIL au DPO de la ville de Nice au sujet du Carnaval, [en ligne](#).

statua en faveur des défenseurs au motif de la préservation des droits de propriété des membres du consortium ayant développé le système¹⁸⁹. Un recours en appel est pendant. De telles pratiques ne sont pas isolées comme le révèle l'étude systématique de C. GARVIE. Dans ces conditions, la dépendance aux opérateurs techniques met à mal les obligations de transparence et d'information des entités et autorités déployant ces systèmes.

b. Les exigences spécifiques en cas de violations des données

-73. Les violations de données (« data breach ») sont caractérisées lorsque les données personnelles sont divulguées accidentellement ou malicieusement. Les articles 33 du RGPD et 30 de la directive police justice prévoient que toute violation doit être notifiée à l'autorité de contrôle, en l'occurrence la CNIL, dans les 72 heures. Le responsable du traitement fait état de la nature des données personnelles affectées, des mesures de garantie initialement appliquées (ex : chiffrement), et des mesures prises pour remédier à cette situation. Selon le directeur de l'ANSSI, une exception peut être admise dans l'hypothèse où la violation a été réalisée par des moyens malicieux, afin d'identifier les hackers.

Cette exception est implicitement prévue par ces deux textes en conclusion de leur premier paragraphe, identique : la notification peut être retardée si elle est « accompagnée des motifs du retard ». Elle est en outre corroborée par les dispositions relatives à l'enquête dans la directive police justice¹⁹⁰. Par ailleurs, la personne concernée est supposée être informée en cas de violation des données. Le contenu de l'information est similaire à celui fourni à l'autorité de contrôle. Des préconisations pour qu'elles puissent en limiter les effets néfastes sont formulées.

-74. Bien que satisfaisante pour le droit commun des données personnelles - où le changement d'un mot de passe ou l'opposition à une carte de crédit sont des solutions faciles – cette procédure n'est pas pleinement satisfaisante en matière de données biométriques. En effet,

¹⁸⁹ CJUE, *Breyer v Commission*, Case T-158/19, 17.6.2019.

¹⁹⁰ Voir en ce sens l'article 31 §5 de la directive justice, relative à la notification des personnes concernées, qui lui-même renvoie au paragraphe 3 de l'article 13 prévoyant explicitement cette exception à la notification de la personne concernée.

comme nous l'avons vu, l'immutabilité de ces données neutralise le degré « d'intervenabilité » de la personne concernée¹⁹¹. Dès lors qu'il n'existe pas de solutions idoines et pleinement satisfaisantes à ces difficultés, le recours aux traitements biométriques doit être d'autant limité.

3. Les garanties techniques et architecturales

-75. Le régime de redevabilité se traduit enfin par l'obligation d'adopter des garanties techniques assurant la sécurité du traitement (a), ainsi que le respect de la vie privée by design et by default (b).

a. La sécurité du traitement

-76. Prévue à l'article 32 du RGPD et à l'article 29 de la directive police justice, la sécurité des traitements de données personnelles constitue une obligation de résultat atténué pour les responsables du traitement, a fortiori pour les catégories particulières de données explicitement visées en conclusion du premier paragraphe de ces deux textes. Ce dernier prévoit une prise en compte de la sécurité des données personnelles en fonction des risques engendrés pour les droits et libertés des personnes physiques pendant toute la durée du cycle de vie des données. Ce degré de risque – extrêmement grave pour les catégories particulières de données – doit entraîner une compréhension élevée de l'état des connaissances pour établir un niveau de garanties en matière de sécurité. Toutefois, comme nous l'avons établi¹⁹², ces systèmes n'offrent pas systématiquement les garanties adéquates et peuvent être usurpés et piratés.

-77. Afin de prévenir ces différents risques l'AIA prévoit, en son article 13 § 3 (ii) l'obligation de transparence du fournisseur de l'IA sur « le niveau d'exactitude, de robustesse et de cybersécurité ». Ce dernier élément est plus précisément décrit à l'article 15, qui prévoit que l'IA doit faire l'objet d'une sécurité informatique renforcée, dès la conception et par défaut, en

¹⁹¹ S. JOYEE De, D. LE MÉTAYER, PRIAM: A Privacy Risk Analysis Methodology. [Research Report] RR-8876, Inria - Research Centre Grenoble – Rhône-Alpes. 2016. [\(hal-01302541\)](#)

¹⁹² Voir *supra* n°29.

fonction de sa fonction. Le premier paragraphe précise que cette exigence doit être maintenue pendant toute la durée d'utilisation de l'IA. Ce même article prévoit un paragraphe spécifiquement dédié aux attaques de tiers en imposant une équivalence entre les circonstances dans lequel s'inscrivent le système d'IA et les mesures de sécurité requises. Enfin dans l'hypothèse où l'IA continue son apprentissage pendant son déploiement, le fournisseur devra prévoir les moyens de préventions sur l'empoisonnement de données¹⁹³ pour éviter, par exemple, la création de discrimination algorithmique. Il est intéressant de relever que les prescriptions de l'AIA sont plus techniques que le RGPD ; ces garanties offriraient aussi un niveau de sécurité accru par rapport au niveau actuel offert.

b. Privacy by design et by default

-78. L'article 25 du RGPD, tel qu'interprété par le CEPD dans ses lignes directrices 4/2019 relatives à la protection des données dès la conception et par défaut¹⁹⁴, contraint le responsable du traitement à prévoir l'implémentation des mesures techniques et organisationnelles appropriées pour optimiser la protection des données personnelles collectées. Cette obligation d'implémentation est d'autant plus importante pour les données sensibles, comme l'atteste, par exemple, l'obligation de réaliser une AIPD. Ainsi, pour répondre aux exigences de la législation européenne, l'expression « **dès la conception** » doit être entendue « de manière efficace et pour intégrer les garanties nécessaires au traitement »¹⁹⁵ et l'expression « **par défaut** » comme la garantie que « seules les données à caractère personnel qui sont nécessaires à chaque finalité spécifique du traitement sont traitées »¹⁹⁶.

-79. La CNIL a eu l'occasion de préciser les implications de ces obligations concernant les systèmes de reconnaissance dans les aéroports¹⁹⁷. Elle recommande dans ce cadre de conserver les données sous le contrôle exclusif de la personne concernée, grâce à l'adoption de deux garanties techniques distinctes :

¹⁹³ C'est-à-dire la « manipulation (du) jeu de données d'entraînement », art. 15§6 du RGPD.

¹⁹⁴ CEPD, Lignes directrices 4/2019 relatives à l'article 25 Protection des données dès la conception et protection des données par défaut Version 2.0 Adoptées le 20 octobre 2020.

¹⁹⁵ Article 25§1. GDPR, article 20§1 de la directive police justice.

¹⁹⁶ Article 25§2. RGPD, Article 20§2 de la directive police justice.

¹⁹⁷ CNIL, Reconnaissance faciale dans les aéroports : quels enjeux et quels grands principes à respecter ?, 9 Octobre 2020.

- D'une part, le contrôle exclusif du passager sur ses données biométriques, lesquelles doivent être stockées sur un support individuel (une application mobile sécurisée sur son téléphone portable, sur un badge, une carte, etc.) ;
- De l'autre, le recours à des bases de données biométriques cryptées, la rendant inutilisable sans l'intervention du passager (grâce à la possession d'un élément ou d'un secret permettant son décryptage, par exemple).

Concernant plus largement les caméras intelligentes, la CNIL invite à implémenter des mécanismes techniques de protection de la vie privée pour réduire les risques. Elle cite à ce titre l'abaissement de la qualité des images¹⁹⁸, le floutage¹⁹⁹, une approche frugale des données²⁰⁰, ou le traitement local des données.

-80. Si les garanties proposées par la CNIL sont techniquement heureuses pour la protection de la vie privée, elles réduisent, cependant, l'efficacité et l'utilité des systèmes. Ces mesures conduisent notamment, en matière d'identification, à des faux positifs. Ainsi, leur implémentation peut neutraliser la finalité même des systèmes, convertissant cet investissement technique en gabegie financière pour les forces de l'ordre. Cela soulève de nouveau la question de l'opportunité des usages des IA physiognomoniques eu égard à leur rapport coût/avantage.

4. Le contrôle humain

-81. Le traitement automatisé des données sensibles est interdit par principe par le RGPD et la directive justice, sauf s'il est autorisé par le droit de l'Union ou des États membres, qui doit prévoir des mesures appropriées pour sauvegarder les droits de la personne concernée²⁰¹. En l'absence de législation spéciale, cela implique un contrôle humain pour tout traitement physiognomonique. Ainsi, une alerte générée par un système automatisé d'identification ne peut conduire à une arrestation automatisée : la décision résultant d'une concordance doit exclusivement reposer sur l'humain. Cette obligation est rappelée à l'article 7 du projet de loi

¹⁹⁸ Susceptible par exemple d'entraîner des faux positifs dans notre cas de figure...

¹⁹⁹ Rendant impossible l'identification d'un criminel dans notre exemple...

²⁰⁰ Empêchant donc l'entraînement de l'algorithme...

²⁰¹ Article 22 RGPD; article 11 de la directive police justice.

sur les Jeux olympiques qui souligne ostensiblement que le système envisagé aura pour seule fonction l'aide à la décision de l'agent assermenté. L'AIA établit également un contrôle humain en son article 14 ; ce contrôle visera à « prévenir ou à réduire au minimum les risques pour la santé, la sécurité ou les droits fondamentaux qui peuvent apparaître lorsqu'un système d'IA à haut risque est utilisé conformément à sa destination ou dans des conditions de mauvaise utilisation raisonnablement prévisible, en particulier lorsque de tels risques persistent ». Le texte prévoit à cet égard deux garanties essentielles :

- L'exigence d'un **contrôle « effectif »**, « par des personnes physiques », pendant la période d'utilisation d'un système d'IA à haut risque. Ce contrôle permet de s'assurer de son adéquate destination, voire de le reconfigurer en cas de mauvaise utilisation voire de l'arrêter.
- L'exigence **d'un niveau de compétence suffisant** pour assurer ce contrôle. En effet, les « personnes chargées d'effectuer un contrôle humain » devront être capables « d'appréhender totalement les capacités et les limites du système d'IA », « d'avoir conscience d'une éventuelle tendance à se fier automatiquement ou excessivement aux résultats produits », « d'interpréter correctement les résultats du système d'IA » et « de décider, dans une situation particulière, de ne pas utiliser le système d'IA à haut risque ».

Le texte prévoit en outre, pour les systèmes d'identification biométrique à distance, qu'aucune mesure ou décision ne pourra être prise par l'utilisateur « sur la base de l'identification résultant du système sans vérification et confirmation par au moins deux personnes physiques ».

-82. Ces garanties sont assurément les bienvenues. Toutefois, les enquêtes de terrain relèvent qu'elles sont rarement suffisantes. Telles sont les conclusions des autorités anglaises concernant les protocoles de déploiement de la reconnaissance faciale²⁰². De même, les travaux déjà cités de C. GARVIE soulignent l'inadaptabilité du contrôle humain dans des systèmes de reconnaissance faciale eu égard aux biais humains²⁰³ que renforcent les

²⁰² MINDEROO CENTRE FOR TECHNOLOGY AND DEMOCRACY, *Audit Scorecard: Assessing police use of facial recognition*, October 27, 2022, [en ligne](#).

²⁰³ Ces biais seraient innés lorsqu'il s'agit d'identifier des visages étrangers et seraient de surcroît renforcés par des biais cognitifs : « A wealth of psychology research demonstrates that overall, humans are not innately good at identifying unfamiliar faces. Error rates range widely, from as low as 10% to higher than 60%, with factors such as image quality, pose variability, age between photographs or similar-looking imposters having a direct impact on

potentiels biais algorithmiques. Pour remédier au problème, l'autrice excipe une étude du Facial Identification Scientific Working Group (FISWG), soulignant qu'une identification judiciaire effective, par des agents, impliquerait une formation de six mois à temps plein²⁰⁴. Un double enseignement peut être tiré de ces études : d'une part, le contrôle humain, pour être effectif, doit être confié à des personnes soumises à une obligation de formation substantielle ; de l'autre, et parfois à défaut, les systèmes d'identification dans les espaces accessibles au public doivent être abandonnés car les risques qu'ils font courir aux personnes concernées ne peuvent être mitigés.

5. La garantie des droits des personnes concernées

a. Les analyses d'impact

-83. Outre les obligations de conformité étudiées, le principe de responsabilité établi par le RGPD et la directive police justice prévoient l'obligation pour le responsable du traitement de réaliser une Analyse d'impact pour la Protection des Données (AIPD) comme condition préalable au déploiement de certains traitements de données personnelles. Compte tenu des éléments factuels et juridiques déjà mentionnés (sensibilité des données traitées, risques, préoccupations du public), l'analyse d'impact apparaît comme un élément procédural essentiel à la mise en œuvre des garanties. Cet outil est conçu comme une preuve de la conformité du processus de traitement des données avec le RGPD et la directive police justice. Elle doit répondre à deux objectifs principaux :

- La définition et l'évaluation des risques pour les données personnelles traitées par le responsable du traitement avant le déploiement d'une opération de traitement, permettant l'atténuation des risques inhérents ;
- La disponibilité d'un outil de gestion de l'évaluation et de prévention des risques, les mesures appropriées pour garantir les droits et les libertés étant classées par ordre de priorité.

accuracy. », C. GARVIE, "A Forensic Without the Science: Face Recognition in U.S. Criminal, Investigations, Center on Privacy & Technology", précédemment cité, p.22.

²⁰⁴ « Following FISWG minimum training and competency requirements would involve six months of full-time, on-the-job training under supervision of a mentor for facial reviewers, operators who are qualified to produce investigative or intelligence leads. It would require 24 months for facial examiners, operators qualified to produce forensic conclusions", Ibidem, p.24.

-84. L'obligation de réaliser une AIPD en amont d'un traitement physiognomonique résulte de l'article 35 du RGPD. Celui-ci dispose en effet que ces analyses sont obligatoires dès lors qu'« un type de traitement, en particulier s'il fait appel à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'entraîner un risque élevé pour les droits et libertés des personnes physiques. » Bien que l'interprétation du caractère « à haut risque » du traitement soit laissée à la seule discrétion des responsables de traitement, l'article 35 §3(b) du RGPD précise que « l'analyse d'impact sur la protection des données (...) est notamment requise en cas de (...) traitement à grande échelle de catégories particulières de données visées à l'article 9, paragraphe 1 ». Le groupe de travail de l'article 29 – devenu le CEDP²⁰⁵ – ajoute que l'AIPD est obligatoire en vertu du RGPD pour certains types de traitement de données. Il fonde son analyse sur neuf critères²⁰⁶ : (1) l'évaluation ou la notation, (2) la prise de décision automatique, (3) la surveillance systématique, (4) le traitement de données sensibles ou de données à caractère hautement personnel, (5) les données à grande échelle, (6) le croisement ou la combinaison d'ensembles de données, (7) les données concernant des personnes vulnérables, (8) l'utilisation innovante ou l'application de nouvelles solutions organisationnelles, et (9) le traitement qui empêche [les personnes concernées] de bénéficier d'un service ou contrat. « Au moins » deux de ces critères quelconques peuvent déclencher la réalisation d'une AIPD²⁰⁷. Or, la plupart d'entre eux se retrouvent dans les systèmes physiognomoniques.

-85. Dans le cadre de la police judiciaire, l'article 27 de la directive police justice, qui prescrit la réalisation d'une AIPD, est moins exhaustif. Seul le considérant 51 indique que « [l]e risque d'atteinte aux droits et libertés des personnes physiques, de probabilité et de gravité variables, peut résulter d'une situation (...) où des données génétiques ou des données biométriques sont traitées afin d'identifier une personne de manière unique ». Bien que les dispositions

²⁰⁵ Groupe de travail de l'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 repris par le CEDP le 25 mai 2018.*

²⁰⁶ Le CEDP évalue ces " situations réglementaires " selon cinq critères distincts, auxquels s'ajoutent quatre nouveaux critères alternatifs. Ces critères sont cumulatifs avec ceux proposés par les ANC sur la base des paragraphes 4 à 6 de l'article 35 du RGPD.

²⁰⁷ N. METALLINOS, « Le principe d'accountability : des formalités préalables aux études d'impact sur la vie privée », *Comm. Com. Elec.*, 2018, dossier 11, interprète ce « au moins » comme le déclenchement par la présence d'un seul critère.

soient moins affirmatives, le sens de la loi semble le même. La CNIL confirme cette interprétation²⁰⁸.

-86. Telles qu'elles sont aujourd'hui prescrites, les AIPD souffrent de diverses lacunes qui pourraient entraver la garantie des droits pour le déploiement des technologies physiognomoniques. Nous insisterons plus particulièrement sur deux d'entre elles : les incertitudes méthodologiques et l'appréciation discrétionnaire du responsable de traitement.

-86a. Le CEPD et l'EDPS ont tous deux opté pour la neutralité méthodologique : ils ne fournissent pas de méthodologie standard²⁰⁹ ni de métriques des risques (indicateurs clés de performance). Ce parti pris engendre des incertitudes quant au périmètre de l'analyse et de l'insécurité juridique²¹⁰. Ainsi, certaines autorités de protection des données européennes comprennent les AIPD comme une « évaluation d'impact sur la vie privée » (PIA)²¹¹ et concentrent leurs préconisations sur l'analyse des risques des « droits et libertés », tandis que d'autres se concentrent davantage sur les risques techniques et les enjeux en termes de cybersécurité²¹². Cela conduit in fine à des niveaux de protection inégaux. L'article 9 de l'AIA ne surmonte pas pleinement ces difficultés. L'article 9 prévoit bien un « système de gestion des risques », inscrivant l'analyse d'impact dans le cycle de vie du système d'intelligence artificielle. Il ne précise toutefois pas le destinataire de cette obligation²¹³ ni la typologie des risques.

-86b. Par ailleurs, l'opportunité de la réalisation d'une AIPD procède de l'évaluation souveraine – discrétionnaire – des risques par le responsable de traitements, que l'absence de

²⁰⁸ CNIL, *Analyse d'impact relative à la protection des données : publication d'une liste des traitements pour lesquels une analyse est requise*.

²⁰⁹ C. LEVALLOIS-BARTH, J. KELLER, *Analyse d'impact relative à la Protection des Données : le cas des voitures connectées*. [Rapport de recherche] Institut Mines-Télécom, Télécom ParisTech, CNRS LTCl. 2021. (hal-03456922)

²¹⁰ L'affaire Ed Bridges l'illustre : alors que le Royaume-Uni était encore soumis aux obligations européennes, une Cour d'appel a jugé que l'AIPD réalisée par la police galloise n'était pas suffisante et « n'était parvenue à évaluer correctement les risques pour les droits et libertés des personnes concernées » ni à « aborder les mesures envisagées pour faire face aux risques » 2020] EWCA Civ 1058 §153.

²¹¹ Notons bien que ces deux évaluations sont différentes et mobilisent des outils distincts. R. CLARKE, *The Distinction between a PIA and a Data Protection Impact Assessment (DPIA) under the EU GDPR, for a Panel at CPDP, Brussels, 27 January 2017*

²¹² C. LEVALLOIS-BARTH, J. KELLER, *Analyse d'impact relative à la Protection des Données*, op cit..

²¹³ Fournisseur ou utilisateur.

méthodologie renforce. Il appartient en effet au responsable d’apprécier la vraisemblance²¹⁴ et la gravité potentielle des dommages²¹⁵ sur les droits et libertés subis par la personne concernée. L’EPDS, considère qu’il s’agit d’une faille, les responsables de traitement n’hésitant pas à minimiser les risques ou mettre délibérément et sciemment de côté certains d’entre eux pour éviter de la réaliser²¹⁶.

b. L’exercice des droits d’information, d’accès et d’effacement

-87. Conformément à l’article 13 du RGPD, les personnes concernées par un traitement sont en droit d’obtenir de la part de son responsable la confirmation que des données à caractère personnel la concernant sont traitées, et peuvent obtenir à ce titre l’accès aux dites données. L’article 12 du RGPD impose au responsable du traitement de faciliter l’exercice de ces droits. Ces dispositions sont essentielles en ce qu’elles permettent, dans l’esprit de la loi, l’exercice d’un contrôle citoyen ; elles sont à cet égard indispensables à la mise en œuvre du régime de redevabilité.

-88. La décision de la CNIL sanctionnant la société Clearview AI le 17 octobre 2022²¹⁷ illustre la problématique²¹⁸. L’autorité française a établi un manquement à l’article 12, constatant que les demandes de la plaignante n’avaient pas abouti. Cette dernière avait envoyé sept courriers recommandés, la copie de sa pièce d’identité sur demande de la partie défenderesse avant de s’engager dans un échange épistolaire de quatre mois. La plaignante n’obtint que des éléments succincts, en l’espèce un résultat de la recherche effectuée par un logiciel et à un renvoi à la politique de confidentialité de la société. La partialité de la réponse, alliée à la difficulté de l’obtenir, est caractéristique des manquements. Ils sont en outre corroborés par une politique de confidentialité que la CNIL condamne en raison de la limitation du droit d’accès qu’elle

²¹⁴ C’est-à-dire la probabilité de la réalisation d’un événement négatif.

²¹⁵ C’est-à-dire l’impact du dommage sur les droits de la personne concernée.

²¹⁶ DPS Survey on Data Protection Impact Assessments, précédemment cité.

²¹⁷ Délibération de la formation restreinte n° SAN-2022-019 du 17 octobre 2022 concernant la société CLEARVIEW AI

²¹⁸ C. LEQUESNE-ROTH, « Mise en demeure de Clearview AI par la CNIL : les jalons d’un combat pour le droit à l’anonymat », précédemment cité.

prescrit : la société restreint l'exercice de ce droit à douze mois, sans démontrer que les données ne sont pas détenues au-delà.

La CNIL a également constaté un manquement au droit à l'effacement encadré par l'article 17 du RGPD qui permet à la personne concernée d'avoir le « droit d'obtenir (...) l'effacement, dans les meilleurs délais, de données à caractère personnel ». L'un des fondements de l'invocation de ce droit est le traitement illicite. La CNIL constate la méconnaissance de ce droit par l'absence de réponse à la demande effectuée par la plaignante.

À la suite d'une mise en demeure restée sans réponse, la CNIL a prononcé une sanction de 20 millions d'euros, et enjoint à la société Clearview AI de cesser de collecter et d'utiliser, sans base légale, les données des personnes se trouvant en France et de supprimer celles déjà collectées.

Toutefois, la société réfute l'autorité de la CNIL, et joue de l'extraterritorialité pour s'y soustraire. Il semble à ce jour impossible de garantir que Clearview AI ait effectivement procédé au retrait des données et arrêté les traitements pour les citoyens français comme exigé.

-89. Cette affaire est riche d'enseignements au regard de l'exercice des droits des personnes concernées. Elle rappelle en premier lieu qu'un système physiognomonique ne saurait être déployé, à des fins de surveillance, sans rendre compte aux citoyens. Sa conclusion invite toutefois à la prudence, car le recours à des sociétés privées étrangères pour déployer ces systèmes affaiblit manifestement en pratique ces mêmes garanties.

C. Les pièges de l'instrumentalisation démocratique : le cas des expérimentations

-90. L'opportunité des expérimentations est fonction du cadre de leur réalisation et de leur objet. Si elles peuvent offrir un recul sur les pratiques, les usages, et les lacunes, c'est à la condition qu'elles soient soumises à un véritable contrôle démocratique tout au long de leur mise en œuvre, en amont comme en aval. « Expérimenter » ne doit pas seulement être entendu comme « tester la technologie », mais comme éprouver un cadre adapté qui offre des

garanties solides en termes de transparence et de redevabilité. L'expérimentation doit nécessairement servir la démocratie technologique ; c'est l'expérience d'un processus démocratique. Des travaux doctrinaux européens sur les « sandboxes » ont mis en évidence l'insuffisante prise en compte de ces considérations²¹⁹. Le risque encouru est celui d'une instrumentalisation de l'expérimentation, qui conduirait à légitimer et institutionnaliser des usages sans cadre adapté, ni assentiment citoyen.

L'expérimentation niçoise lors du Carnaval de 2019 est à cet égard riche d'enseignements et montre l'inadaptation de la loi pour conduire ces expérimentations :

- En amont, on peut regretter *l'absence de mandat de la CNIL pour « autoriser »* la ville à mener cette expérimentation. En l'espèce celle-ci a été source d'insécurité juridique et d'atermoiements dommageables pour l'ensemble des parties (ceux qui conduisaient l'expérimentation, comme ceux qui étaient visés). In fine, et en l'absence de directives claires, l'autorité de protection des données elle-même s'est déclarée insatisfaite du déroulé de l'expérimentation.
- La ville n'a pas été en mesure de fournir les éléments tenant aux *spécificités techniques* du protocole déployé, notamment concernant les biais, ces informations relevant en toute vraisemblance du secret industriel de l'opérateur technique. Ici encore, le régime de redevabilité applicable aux tiers n'étant pas clairement défini, les exigences de transparence qu'une expérimentation doit servir ne sont pas remplies.
- L'évaluation quant à l'acceptabilité du dispositif a été produite par la ville elle-même. La position de « juge et partie » n'est pas satisfaisante quant à la probité des résultats obtenus et met en évidence la nécessité d'impliquer des *tiers impartiaux*.

Notons en outre que bien que les expérimentations soient courantes²²⁰, et souvent présentées comme une panacée démocratique, elles ne disposent pas davantage de fondement légal²²¹.

²¹⁹ S. RANCHORDAS, "Experimental Regulations and Regulatory Sandboxes: Law without Order?" (September 30, 2021), University of Groningen Faculty of Law Research Paper No. 10/2021, <http://dx.doi.org/10.2139/ssrn.3934075>

²²⁰ New Surveillance Technologies in Public Spaces – op cit.

²²¹ Il convient en outre de relever que le cadre expérimental est soumis au RGPD, comme à la directive police justice : les expérimentations ne font pas l'objet de dispositions plus souples. Exception faite des authentifications (réalisées sur la base du consentement), les fondements légaux sont mal adaptés, voire défectueux, pour permettre (et justifier) le déploiement de la reconnaissance faciale à des fins d'identification dans les espaces accessibles au

La réflexion sur les conditions d'exercice apparaît ainsi tout aussi nécessaire et s'inscrit dans celle, plus large, de la mise en place des contrôles démocratiques.

-91. La procédure envisagée par la loi d'expérimentation pour les JO 2024 n'offre pas, au regard de ces éléments d'analyse, les garanties démocratiques attendues. L'article 7 prévoit que la procédure s'articulera en trois temps : le déploiement sera autorisé par voie de décret, pris après réalisation d'une AIPD et avis de la CNIL ; les outils seront, dans un second temps, développés par l'État ou un tiers « sous le contrôle d'une autorité compétente délivrant une « attestation de conformité » rendue publique²²² ; enfin, l'expérimentation fera l'objet d'une autorisation « expresse et écrite délivrée par le préfet du département ou à Paris le préfet de Police ». Elle sera nécessairement accompagnée de l'AIPD actualisée, puis transmise à la CNIL.

Il est important de relever que l'autorité de protection des données est en l'espèce cantonnée au modeste rôle d'observateur. Elle n'est en mesure d'exercer aucun contre-pouvoir effectif : il ne lui revient pas d'autoriser les déploiements – son avis est purement consultatif - et ne peut davantage les suspendre en cas de manquement au droit de la protection des données ou aux libertés fondamentales. Les amendements proposés dans le cadre des débats parlementaires envisagent de renforcer son implication dans le processus d'élaboration des traitements (phase 2) ; notons que ces propositions apparaissent en outre assez déconnectées de la réalité dans l'hypothèse du recours (récurrent) à des prestataires extérieurs²²³.

public (voir *supra* n°39 et suivant). Aussi, même sur le terrain expérimental, une loi apparaît nécessaire

²²² Le législateur semble ici se référer à la mécanique de certification prévue par l'AIA.

²²³ Voir *supra* n°71, le contentieux relatif au refus d'accès à la documentation du système au nom du secret des affaires portées devant la CJUE.



IV. Pour un régime de redevabilité adapté

-92. L'encadrement des usages des technologies d'identification alimente l'actualité sociale et juridique depuis plus de deux ans : de la reconnaissance faciale à la vidéosurveillance, la production de rapports et de propositions en écho à la dynamique européenne, en témoigne. Il est important de souligner que le droit peut et le législateur doit²²⁴ intervenir. Il en va de la sécurité juridique, et plus largement, de la démocratie. La juridicisation des enjeux éthiques apparaît en outre indispensable pour éviter l'instrumentalisation des chartes éthiques et autres « bonnes pratiques ». L'histoire récente des technologies témoigne de ces dérives²²⁵ : elles induisent un biais d'acceptabilité, qui pourrait conduire à desserrer la contrainte réglementaire et institutionnaliser, in fine, des pratiques démocratiquement contestables. La présente étude a permis de dresser plusieurs constats :

- Les IA d'identification dites « IA physiognomoniques » (reconnaissance faciale, émotionnelle et comportementale) ont fait l'objet de nombreux *travaux scientifiques* et suscitent *un intérêt accru de la part des forces de l'ordre* ;
- En parallèle, elles continuent à alimenter les craintes du public au regard des *risques d'atteintes aux droits fondamentaux* auxquelles elles exposent les personnes

²²⁴ L'article 34 de la Constitution française ne laisse pas place à l'ambiguïté : la protection des libertés publiques, en jeu dans le cadre de la mobilisation des outils de reconnaissance faciale, impose une intervention du législateur. L'exhaustivité (concernant notamment la finalité des usages et l'ouverture de recours) et la spécificité des garanties apportées conditionneront d'ailleurs la constitutionnalité du régime établi. Tel est également le sens de la jurisprudence européenne. En ce sens : C. LEQUESNE ROTH, « De la fin de l'anonymat : reconnaissance faciale et droit à la vie privée », *Dalloz IP/IT*, Juin 2021, pp. 308-313.

²²⁵ Ainsi, les prises de position de certains géants du numérique, pour louables qu'elles soient, annonçant la suspension de leurs activités en matière de reconnaissance faciale ou plus récemment, d'une reconnaissance faciale dite « éthique », « AnyVision proposes three ethical facial recognition principles for police », *Biometric Update*, Sep 8, 2021 [en ligne](#).

concernées : risque d’atteinte à la vie privée, à la liberté d’expression, d’association, d’aller et venir. Les risques sont d’autant plus significatifs que ces systèmes procèdent à des traitements de données sensibles – les données biométriques – qui se caractérisent par leur immuabilité. Le vol de données biométriques ouvre la voie à une usurpation d’identité, qui offre peu de solutions (contrairement au vol de codes d’accès). Les risques inhérents à ces technologies se posent ainsi, également, sur le terrain de la **sécurité et de la souveraineté des données**.

- En termes de déploiement, l’offre industrielle ne rencontre pas les attentes du secteur public de la surveillance en raison d’un cadre juridique et procédural encore incertain. En sus de **fondements légaux lacunaires**, l’analyse révèle que le **régime de redevabilité** n’est pas adapté aux risques identifiés.
- Les propositions légales en cours (Artificial Intelligence Act à l’échelon européen et Loi d’expérimentation pour les JO 2024 à l’échelon national) apportent de premiers éléments de réponse sans toutefois résoudre l’ensemble des difficultés identifiées :
 - o L’AIA offre une base légale au déploiement des technologies d’identification à des fins de surveillance dans les espaces accessibles public ; la proposition renvoie toutefois la balle aux législateurs pour élaborer les procédures de déploiement indispensables au respect des garanties constitutionnelles et conventionnelles ;
 - o La loi d’expérimentation pose les premiers jalons de ces procédures pour la vidéosurveillance dite intelligente. Elle peine toutefois à identifier les risques et n’instaure aucun contrepouvoir substantiel, ceux-ci étant concentrés dans les mains de l’exécutif.

Les présentes recommandations visent à compléter l’arsenal législatif pour renforcer les conditions de la démocratie technologique.

1. Limiter strictement les usages de l’IA physiognomonique

-93. Eu égard aux risques que ces technologies soulèvent en termes de sécurité et de droits fondamentaux (surveillance de masse), leur usage par les forces de l’ordre doit être substantiellement restreint. Dans le prolongement de l’AIA (article 5), nous plaçons pour le

maintien strict de leur interdiction à des fins d'identification *en temps réel dans les espaces accessibles au public*. Le champ de ces *exceptions* doit aussi être strictement limité et circonscrit. L'AIA paraît à cet égard trop large et réduit substantiellement la portée de l'interdiction.

-94. Concernant la reconnaissance faciale, les exceptions renvoient aux infractions pénales visées à l'article 2, paragraphe 2, de la décision-cadre 2002/584/JAI du Conseil qui intègrent, notamment, des infractions de nature économique. Celles-ci nous semblent devoir être écartées et concerner uniquement les *crimes* menaçants – ou portant atteinte – à *l'intégrité physique* des personnes. Une nouvelle fois, au regard des risques que comporte la technologie, *la proportionnalité des moyens* impose que l'usage de la reconnaissance faciale ne puisse faire l'objet d'aucune autre alternative.

Comme précédemment souligné, les distinctions opérées entre authentification et identification apparaissent justifiées au regard des *risques* encourus. Les opérations d'identification doivent faire l'objet d'un encadrement plus strict.

L'exigence de proportionnalité exclut ainsi, à notre sens, l'usage de la reconnaissance faciale à *des fins d'identification*, lequel doit *formellement être interdit en certains domaines à l'instar des écoles, des établissements d'enseignement, et sur les lieux de travail*.

En outre, le respect des principes de proportionnalité et de nécessité impose que le recours à l'identification faciale automatisée soit strictement circonscrit (notamment dans le temps et l'espace) et subordonné à des circonstances exceptionnelles (risques pour la sécurité et l'intégrité des personnes).

2. Identifier les autorités compétentes

-95. La question des autorités pertinentes et de leurs moyens constitue un élément essentiel du régime de redevabilité qui sera mis en place (de son efficacité et de son effectivité).

La proposition de règlement européen sur l'intelligence artificielle a initié un débat, déjà entamé par la doctrine, concernant les autorités de contrôle en matière des systèmes intelligents. La proposition prévoit en effet, dans son modèle de gouvernance, l'instauration d'autorités nationales dédiées. Au regard de l'articulation que supposera le droit de la protection des données à caractère personnel et ce droit en cours d'adoption, la **Commission Nationale Informatique et Libertés (CNIL)** semble désignée pour assurer les missions d'accréditation et de contrôle. Elle s'est d'ailleurs prononcée en ce sens dans le cadre d'un avis conjoint avec ses homologues européens²²⁶.

Cette proposition nous semble bienvenue sous réserve que la CNIL soit **dotée des moyens financiers, humains et techniques supplémentaires** pour assurer ces nouvelles missions. La question des contrôles conjoints entre autorités - combinant par exemple, du contrôle technique pur à des contrôles juridiques - devra en outre être soulevée et clairement établie.

-96. En ce qui concerne l'usage des technologies d'identification **par les forces de l'ordre**, il apparaît nécessaire de concevoir différents contrôles en fonction de deux paramètres : la temporalité du déploiement (autorisation/contrôle a posteriori des usages) et les pouvoirs de police concernés (police administrative/police judiciaire).

Dans le cadre préventif (**police administrative**), les autorisations de déploiement - qui concerneraient la surveillance exceptionnelle d'un espace accessible au public - pourraient être délivrées par la **CNIL**. Celle-ci veillerait également au respect du protocole défini, et contrôlerait a posteriori les usages mis en œuvre. Il serait, à cet égard, souhaitable que soit distingués en son sein les agents (voire les cellules), dédiés aux accréditations de ceux dévolus au contrôle a posteriori.

Dans le cadre répressif (**police judiciaire**), et conformément au droit de la procédure pénale, le pouvoir d'autorisation devrait être dévolu au **juge judiciaire**.

²²⁶ « [L]a CNIL considère que les autorités de protection des données devraient être désignées comme autorités de contrôle nationales de l'intelligence artificielle ». CNIL, *Intelligence artificielle : l'avis de la CNIL et de ses homologues sur le futur règlement européen*, 8 juillet 2021, en ligne : <https://www.cnil.fr/fr/intelligence-artificielle-lavis-de-la-cnil-et-de-ses-homologues-sur-le-futur-reglement-europeen>

-97. En parallèle, il apparaît aujourd'hui indispensable de faire évoluer les **contrôles internes des agents** à l'aune de l'évolution de l'équipement technologique des forces de l'ordre. Au-delà même de la reconnaissance faciale, l'introduction d'outils d'intelligence artificielle (de type police prédictive) appellent une vigilance particulière concernant la formation des agents dépositaires de l'ordre public, leur habilitation à les utiliser et le contrôle de leur pratique.

Le législateur pourrait à cet effet faire preuve d'innovation en s'appuyant sur les structures existantes. Pourraient ainsi être instituées, au sein de l'Inspection Générale de la Police Nationale (IGPN) et l'Inspection Générale de la Gendarmerie Nationale (IGGN) des **cellules « Tech »**, composées d'ingénieurs et de juristes, chargées de conduire des missions d'audit.

3. Autoriser et contrôler

-98. Dans la perspective de l'instauration d'un régime pérenne, nous plaidons pour l'instauration d'un **régime d'autorisation préalable** « bicéphale » en fonction des pouvoirs de police concernés (police administrative/police judiciaire) et un **régime de contrôle a posteriori** veillant à la conformité des usages.

Conformément à la jurisprudence constitutionnelle et européenne, tout déploiement de la technologie à des fins d'identification devra être **limité** :

- Dans le cadre préventif (en temps réel): dans le temps (événement présentant un risque pour le maintien de l'ordre), dans l'espace (périmètre concerné) et désigner expressément les personnes habilitées à son emploi.
- Dans le cadre répressif (reconnaissance a posteriori), à la demande formulée auprès du juge judiciaire.

Nous plaidons, à cet égard, pour l'assimilation des recherches par reconnaissance faciale à des **actes d'information ou d'instruction**.

Outre les principes de nécessité et proportionnalité, et dans la ligne de l'AIA (article 5), l'autorisation devra nécessairement être subordonnée au déploiement d'un **protocole dédié** précisant les garanties adoptées et adaptées concernant notamment :

- L'information du public ;
- La minimisation des données (données conservées, temps de conservation) ;
- La supervision humaine (système de vérification des résultats engendrés par les systèmes) ;
- La sécurité des données (l'usage de solutions commerciales telles que celles offerte par Clearview, outre le caractère illégal de ce traitement, est considéré comme techniquement risqué) ;
- La traçabilité des données ;
- Les modalités des processus d'évaluation et les exigences de compte rendu ex-post (relatif, notamment, aux erreurs techniques et au biais comme demandé la CNIL à l'issue de l'expérimentation niçoise).
- Le protocole devra également préciser les finalités du traitement, les dates de déploiement du dispositif et les personnes habilitées à solliciter des requêtes.
- La désignation des agents compétents, sur la base d'une formation adaptée.

-99. Ces éléments apparaissent d'autant plus essentiels que l'AIA dessine une délégation normative au bénéfice du secteur privé au travers d'un système de certification contestable. En effet, la procédure de mise en conformité des systèmes prévue à l'article 43-1 de l'AIA – dont relèverait les systèmes d'identification faciale compris comme « systèmes à haut risque » – sera(it) dans une large mesure dévolue à ces organismes. Il appartiendra(it) à ces derniers d'établir la méthodologie et les normes d'évaluation. Ce modèle confère(rait) un rôle d'importance majeure à des acteurs privés (régulation de l'accès au marché et normes de conformité). L'imposition de protocoles, et d'audits propres à l'administration publique apparaît, à cet égard, d'autant plus décisive.

4. Reconnaître la normativité des actes numériques

-100. La normativité des usages – des actes – numérique de l’administration et des forces de l’ordre n’est aujourd’hui nullement prise en compte²²⁷. Il est impératif que la normativité des recherches effectuées avec ces logiciels soit reconnue. Le rapport de contrôle de l’Organe belge de contrôle de l’information policière déjà mentionné révèle à ce titre des pratiques préoccupantes du point de vue de l’état de droit. Il relève que l’usage des outils de reconnaissance faciale est apparenté, au sein des forces de police belge, à une recherche sur un moteur Internet. Ces traitements ont souvent lieu pendant la phase préalable à une ouverture ou une instruction et ne sont « nulle part saisis ni journalisés dans les banques de données policières existantes »²²⁸. Ces traitements biométriques sont dès lors réalisés en dessous des « radars juridiques » et donc des impératifs démocratiques.

Il nous paraît aussi indispensable que l’usage de la reconnaissance faciale soit assimilé, dans le cadre des procédures pénales, à *des actes d’information ou d’instruction*, et soumis à un régime procédural identique.

5. Renforcer le devoir d’information

-101. Par ailleurs, et dans le même sens, les forces de l’ordre devraient être tenues à un *devoir d’information* à l’égard des personnes concernées dès lors qu’elles font usage de ces technologies. Pour être effective, l’information doit être multi-niveaux et multi-supports. Lors des expérimentations conduites au Royaume-Uni dans les espaces accessibles au public, les organisations non gouvernementales ont mis en évidence qu’en dépit des efforts des autorités, la signalétique était insuffisante pour permettre aux personnes concernées d’exercer leurs droits (alternative quand les expériences étaient fondées sur le consentement), et de comprendre les enjeux. La Cour d’appel qui s’est prononcée sur l’usage de la reconnaissance faciale par la police du Pays de Galles a confirmé cette analyse : le triple dispositif déployé (informations sur les réseaux sociaux, les véhicules de police et distribution de flyers) ne

²²⁷ Conseil constitutionnel, 12 juin 2018, n° 2018-765 DC, Loi relative à la protection des données personnelles.

²²⁸ [Rapport DIO21006](#), Février 2022.

suffisait pas à prévenir les atteintes au droit de la vie privée constatées²²⁹. Le devoir d'information doit aussi faire l'objet d'un protocole (déployé par l'autorité de contrôle ou en collaboration avec celle-ci dans le cadre des expérimentations). À défaut, le risque est celui d'une « banalisation » de ce droit au mépris de l'acceptabilité sociale à laquelle il doit contribuer.

6. Approfondir les analyses d'impact

-102. Nos analyses ont mis en évidence les lacunes liées à aux analyses d'impact. Elles résultent de la conjonction entre l'absence d'obligation expresse et le caractère discrétionnaire de la méthode (l'opportunité de leur réalisation et l'identification des risques relève de l'appréciation de seul responsable de traitement).

Pour renforcer la transparence des usages, le législateur devrait consacrer ***l'obligation de publier l'analyse d'impact relative à la protection des données (AIPD)*** réalisée en amont du déploiement de ces technologies. Tout utilisateur d'un système d'identification dans les espaces accessibles au public devrait être tenu de soumettre son AIPD à la CNIL en amont de tout déploiement, pour permettre un contrôle effectif.

A minima, le responsable du traitement devrait être tenu de publier un résumé clair, accessible aux néophytes. Celui-ci comprendrait, sous une forme intelligible :

- l'ensemble des décisions ou des situations faisant l'objet d'un traitement automatisé,
- les critères intervenant dans une décision,
- les informations sur les données utilisées,
- une description de la méthode utilisée pour la collecte de données.

Pour préserver certains secrets des affaires, ce résumé pourrait être expurgé de tous les éléments techniques pour se concentrer uniquement sur le type de données collectées et leur traitement précis.

²²⁹ [2020] EWCA Civ 1058 §20.

Cette communication offrirait tant au public concerné qu'à la CNIL un moyen de contrôle supplémentaire.

Nous encourageons également le législateur à rendre cette **consultation juridique préalable de l'utilisateur d'une IA physiognomoniques payante**, pour permettre à la CNIL de se doter les moyens humains et techniques pour exercer ce contrôle.

-103. Nous invitons parallèlement le législateur à préciser **la méthodologie des AIPD relatives aux IA physiognomoniques** de la façon suivante :

- L'analyse devra porter principalement sur la vraisemblance des risques en répondant aux exigences de sûreté, de sécurité et de robustesse dès la conception ;
- L'examen devra effectuer une analyse d'impact s'assurant que certaines caractéristiques telles que le genre ou la couleur de peau sont exclues, pour éviter les discriminations illégales ;
- L'analyse devra notamment identifier les impacts négatifs potentiels du système de traitement sur les droits de l'homme en documentant toutes les évolutions du modèle ;
- L'analyse devra être contrôlée, à l'instar de ce qui est fait dans le domaine financier, par deux entités privées concurrentes pour s'assurer de la sincérité des résultats ;
- L'analyse réalisée devra enfin voir son résumé être communiqué soit au journal officiel, soit dans un bulletin municipal officiel.

7. S'interroger quant au régime de consentement

-104. Force est de constater une différence d'acceptabilité et de régime entre les usages individuels des IA d'identification (déverrouillage des smart phones, entretien d'embauche) et leurs usages dans les espaces accessibles au public ; cela tient notamment aux finalités distinctes des traitements (surveillance individuelle v./surveillance publique). **Aussi, les fondements juridiques des traitements ne sont – et ne peuvent pas être – les mêmes.**

Pour autant, il est vrai que les deux régimes entrent en collision : comment justifier que la reconnaissance faciale soit admise pour déverrouiller nos téléphones et non pour faciliter la recherche d'un enfant perdu dans des conditions très restrictives ?

Cet écueil appelle à penser de concert les deux régimes.

Au regard des risques déjà évoqués, *le régime de consentement* (qui caractérise principalement les usages privés) doit être mis en cause dans certains cas, comme dans le cadre professionnel pour prévenir des rapports de force inégaux et des usages disproportionnés. En parallèle, le régime public doit être conçu et construit autour d'usages restreints apportant de fortes garanties en matière de contrôle et de redevabilité. L'acceptabilité sociale sera en grande partie fonction de celles-ci : la transparence des autorités, l'information du public et les contrôles établis apparaissent à cet égard indispensables.

TABLE DES MATIÈRES

Remerciements	7
Sommaire	9
Liste des abréviations	11
INTRODUCTION. Des jeux olympiques au « panopticon »	13
I. Technologies de surveillance, IA physiognomonique : qu'est-ce à dire ?	17
A. Reconnaissance faciale	17
B. Vidéo surveillance dite « intelligente »	22
C. L'hypothèse de l'IA physiognomonique	29
II. De la maturité technologique à l'acceptabilité sociale : les risques de l'IA physiognomonique	31
A. Dysfonctionnements technologiques et état de droit	32
1. <i>Les atteintes aux droits fondamentaux résultant des biais algorithmiques</i>	32
2. <i>Sécurité des données et souveraineté numérique</i>	38
B. Technologies de surveillance contre les libertés	42
1. <i>Surveillance généralisée et atteinte à la vie privée</i>	42
2. <i>Liberté d'expression, de croyance et d'assemblée et le <u>chilling effect</u></i>	44
III. Les lacunes des régimes applicables aux technologies physiognomoniques	47
A. L'absence de fondements légaux adaptés	48
1. <i>Les fondements communs aux régimes administratifs et judiciaire</i>	49
a. <i>La sauvegarde des intérêts vitaux</i>	49
b. <i>Les données manifestement rendues publiques</i>	50
c. <i>Le droit de l'Union ou du droit d'un État membre</i>	51
2. <i>Les fondements propres au régime administratif</i>	54
a. <i>Le consentement</i>	54
b. <i>L'exécution d'un contrat</i>	55
B. Les garanties incertaines du régime en vigueur	56
1. <i>Les garanties dues au titre de la protection des données</i>	56
a. <i>Légalité et nécessité du traitement</i>	56
b. <i>Définition des finalités du traitement</i>	57
c. <i>Proportionnalité des traitements</i>	57
d. <i>Minimisation des données</i>	59
e. <i>Exactitude des données</i>	59
f. <i>Conservation des données</i>	60
2. <i>Les garanties liées au responsable du traitement</i>	61
a. <i>Obligations de transparence et d'information</i>	61
b. <i>Les exigences spécifiques en cas de violations des données</i>	64
3. <i>Les garanties techniques et architecturales</i>	65
a. <i>La sécurité du traitement</i>	65
b. <i>Privacy by design et by default</i>	66
4. <i>Le contrôle humain</i>	67

5. <i>La garantie des droits des personnes concernées</i>	69
a. <i>Les analyses d'impact</i>	69
b. <i>L'exercice des droits d'information, d'accès et d'effacement</i>	72
C. Les pièges de l'instrumentalisation démocratique : le cas des expérimentations	73
IV. Pour un régime de redevabilité adapté	77
1. <i>Limitier strictement les usages de l'IA physiognomonique</i>	78
2. <i>Identifier les autorités compétentes</i>	79
3. <i>Autoriser et contrôler</i>	81
4. <i>Reconnaître la normativité des actes numériques</i>	83
5. <i>Renforcer le devoir d'information</i>	83
6. <i>Approfondir les analyses d'impact</i>	84
7. <i>S'interroger quant au régime de consentement</i>	85

CRÉDITS

Mise en page : Anaïs Rebuccini (Observatoire de l'éthique publique)

Images : sauf mention contraire, toutes les images utilisées dans ce document sont libres de droits et diffusées sous licence adobe stock



LIVRE BLANC POUR L'OBSERVATOIRE DE L'ÉTHIQUE PUBLIQUE

Surveiller les foules

POUR UN ENCADREMENT DES IA
« PHYSIOGNOMONIQUES »

<https://www.observatoireethiquepublique.com/>

IEP de Lille - 9 Rue Auguste Angelliers - 59000 LILLE

E-mail : contact@observatoire-ethique-publique.com

Twitter : @ObservatoireEP

LinkendIn : L'Observatoire de l'Ethique Publique