MASTER COMPLÉMENTAIRE EN DROIT DES TECHNOLOGIES NOUVELLES

« 1984 » en 2024 ? L'encadrement par le droit de la protection des données à caractère personnel et l'AI Act de la vidéosurveillance algorithmique et de son expérimentation aux Jeux olympiques et paralympiques de Paris 2024.

Nardi, Aline

Award date:
2023

Awarding institution:
Universite de Namur

Université de Namur

Faculté de droit

« 1984 » en 2024 ?

L'encadrement par le droit de la protection des données à caractère personnel et l'*AI Act* de la vidéosurveillance algorithmique et de son expérimentation aux Jeux olympiques et paralympiques de Paris 2024.

Mémoire réalisé par :

Aline NARDI

Sous la supervision de :

Elise DEGRAVE

Florian JACQUES

Master DTIC **Année académique 2022-2023**

Engagement de non-plagiat

Le plagiat est considéré comme une fraude et est sanctionné en conséquence.

Est notamment considéré comme plagiat le fait :

- de copier textuellement un passage d'un livre, d'une revue ou d'une page web sans le mettre entre guillemets et sans en mentionner la source ;
- d'insérer dans un travail des images, des graphiques, des données, etc. provenant de sources externes sans en indiquer la provenance ;
- de résumer ou de paraphraser l'idée originale d'un auteur en l'exprimant dans ses propres mots, en omettant d'en indiquer la source ;
- de traduire un texte sans mettre de guillemets autour du passage traduit et sans en mentionner la provenance ;
- d'utiliser le travail d'une autre personne et de le présenter comme le sien (même si cette personne a donné son accord).

Que l'on cite, que l'on résume ou que l'on paraphrase (réécriture complète des passages exploités, avec transformations syntaxiques et lexicales), il faut toujours référencer.

Tenant compte de quoi, en tant qu'auteur du présent travail, je garantis que ce travail ne contient aucune forme de plagiat.

Article 36, § 3, du Règlement des Etudes et des Examens : « §3. En cas de fraude avérée [= plagiat] ou de manquement au respect des consignes, le jury peut attribuer la note de 0/20 à l'unité d'enseignement concernée et ce, même si les faits se sont déroulés lors d'un[e] […] évaluation portant sur une partie de l'unité d'enseignement concernée et dont le résultat constitue un élément de la note globale.

Par ailleurs, le jury peut prendre à l'égard de l'étudiant fraudeur, toute sanction académique qu'il juge utile telle que l'attribution de la note de 0/20 à l'ensemble ou à une partie des épreuves de la période d'évaluation, l'interdiction de poursuivre la période d'évaluation, l'interdiction de s'inscrire à la (ou aux) période(s) d'évaluation suivante(s) ou l'interdiction de participer à certaines évaluations. »

« Bien sûr, il n'y avait aucun moyen de savoir si on était observé à tel ou tel moment. À quelle fréquence et selon quelle règle la police de la pensée se branchait sur un réseau individuel, on ne pouvait que le deviner. Il était même possible qu'elle surveille chacun en permanence. En tous cas, elle pouvait se connecter sur votre réseau à tout moment. On devait vivre, on vivait – par une habitude qui s'était muée en instinct – en partant du principe que le moindre son était écouté et, hormis dans l'obscurité, le moindre mouvement épié. »

G. ORWELL, *1984*, trad. C. IZOARD, *s.l.*, Éditions de la rue Dorion, 2019, p. 17 et 18.

INTRODUCTION

1 À l'approche des Jeux olympiques et paralympiques, qui prendront place en 2024 à Paris (ci-après « les JO 2024 »), la France se prépare à des menaces sécuritaires d'origine multiple. Du terrorisme à la délinquance, en passant par les dangers NRBCe (Nucléaire, Radiologique, Biologique, Chimique et Explosif), le gouvernement français ne veut prendre aucun risque[1]. Pour assurer la sécurité des jeux, une loi autorisant l'expérimentation de technologies de vidéosurveillance algorithmique (ci-après « la VSA ») a récemment été adoptée[2]. À la croisée entre la vidéosurveillance et l'intelligence artificielle (ci-après « l'IA »), ces dernières promettent de révolutionner le travail des forces de l'ordre, notamment en détectant automatiquement des objets abandonnés, surveillant les foules, et reconnaissant des comportements « anormaux » ou le visage de personnes fichées.

2 Le projet de cette loi avait déjà suscité de vives inquiétudes de la part de la société civile, dénonçant « une grave menace pour les libertés civiques et les principes démocratiques », en particulier le droit à la protection des données[3]. L'objet de la présente étude est donc d'étudier les technologies de VSA déployées dans les espaces accessibles au public par des autorités publiques, en particulier celles envisagées pour la sécurisation des JO 2024, et leur conformité au cadre juridique relatif au droit de la protection des données à caractère personnel ainsi qu'un potentiel encadrement par le futur règlement sur l'IA[4] (ci-après « l'*AI Act* »).

3 En particulier, il s'agira premièrement de tracer les contours de la VSA, en présentant ses applications, ses avantages, ses risques et son expérimentation dans le cadre de la surveillance des JO 2024 (Titre I). Dans un deuxième temps, nous analyserons l'alignement de la VSA, en illustrant notre propos au moyen de la loi française, par rapport au droit de l'Union européenne (ci-après « l'UE ») relatif à la protection des données à caractère personnel, au travers de l'article 8 de la Charte des droits fondamentaux de l'UE[5] (ci-après « la Charte »), ainsi que le Règlement général sur la protection des données[6] (ci-après « le RGPD ») et la directive dite « police-justice »[7] (Titre II). Enfin, les technologies de VSA reposant sur l'IA, nous examinerons la pertinence et la portée de certaines garanties présentes dans le projet de l'*AI Act* pour l'encadrement futur des technologies de VSA (Titre III).

---

[1] J.-M. LECLERC, « JO 2024 : Gérald Darmanin veut un dispositif sécuritaire digne d'un événement planétaire », *Le Figaro*, 26 octobre 2022.

[2] L. n°2023-380, 19 mai 2023, relative aux jeux Olympiques et Paralympiques de 2024, NOR : SPOX2233026L, art. 10.

[3] HUMAN RIGHTS WATCH, « Lettre de la société civile aux députés français sur le projet de loi relatif aux Jeux olympiques et paralympiques 2024 », disponible sur https://www.hrw.org/fr, 7 mars 2023.

[4] 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, 21 avril 2021.

[5] Charte des droits fondamentaux de l'Union européenne, *J.O.C.E.*, C 364, 18 décembre 2000.

[6] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), *J.O.U.E.*, L 119, 4 mai 2016.

[7] Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, *J.O.U.E.*, L 119, 4 mai 2016.

Titre I. LES CONTOURS DE LA VSA : CADRE THÉORIQUE ET CAS D'ÉTUDE DES JO 2024

La notion de VSA renvoie à diverses technologies d'IA de traitement d'images, destinées à des usages variés. Il est donc impératif d'établir les contours de cette notion (Chapitre 1) et d'en concrétiser la portée à l'appui d'un cas d'étude d'actualité, tel que l'expérimentation de la VSA pour les JO 20224 (Chapitre 2), afin de mieux appréhender les enjeux que le déploiement de ces technologies représente. 4

Chapitre 1. Cadre théorique

La VSA est un ensemble de technologies complexes, recouvrant des réalités différentes selon l'application qui est faite des « caméras intelligentes » (Section 1). Son déploiement dans les espaces publics présente des avantages (Section 2) et des risques pour les citoyens (Section 3), qu'il convient de soulever avant d'étudier son encadrement par la législation actuelle et future. 5

Section 1. La notion et les applications de la VSA

La VSA ou l'expression caméras « intelligentes » désignent des technologies automatisant l'analyse, *a posteriori* ou en temps réel, d'images issues de la vidéosurveillance[8]. Celles-ci utilisent des logiciels basés sur la technologie de la *computer vision* (vision par ordinateur), permettant de traiter des images numériques fixes ou animées et d'en extraire des données afin de produire un résultat, comme mettre en évidence des caractéristiques spécifiques tirée des images ou encore formuler des recommandations sur la base de celles-ci[9]. Pour ce faire, les technologies de *computer vision* ont recours à l'intelligence artificielle et plus précisément, à l'apprentissage statistique, une forme d'apprentissage automatique généralement supervisé[10]. Une étape essentielle de cet apprentissage est celui de la détection d'images, durant laquelle les algorithmes sont entraînés à détecter automatiquement des informations ciblées[11]. 6

La VSA connait de nombreuses applications. Seules celles déployées dans le cadre de la surveillance des espaces accessibles au public et en particulier, celle des JO 2024, font l'objet de cette étude. À ce titre, plusieurs utilisations peuvent d'ores et déjà être épinglées. La VSA est employée dans la surveillance des objets, en particulier leur détection, leur comptage, leur suivi et l'analyse de leurs trajectoires. Ceci couvre notamment le suivi des véhicules et l'analyse du trafic, ainsi que la détection de fumée et incendies, ou encore la détection des objets abandonnés ou emportés. Elle peut également être destinée à la surveillance des individus, des foules et des comportements. Peuvent ainsi être détectés et analysés : la présence de silhouettes humaines, une violation d'un périmètre, le vandalisme des caméras, le comportement des foules, la reconnaissance d'activités et de comportements, ainsi que l'identification de comportements « anormaux », tels que les bagarres, les évanouissements et les chutes[12]. Notons que la VSA ne vise pas nécessairement l'identification des personnes à titre individuel, même si certaines de ces applications le pourraient, comme la reconnaissance faciale[13], située à la croisée des chemins entre la VSA et les technologies biométriques. 7

---

[8] C. LEQUESNE ROTH et J. KELLER, « Livre blanc pour l'Observatoire de l'éthique publique : surveiller les foules, pour un encadrement des IA 'physiognomoniques' », disponible sur https://www.observatoireethiquepublique.com, 1er avril 2023, p. 22.

[9] IBM, « Qu'est-ce que la Computer Vision ? », disponible sur https://www.ibm.com, *s.d.*, consulté le 7 juin 2023.

[10] X, « Théorie de l'apprentissage statistique », disponible sur https://fr.wikipedia.org, *s.d.*, consulté le 7 juin 2023.

[11] IBM, *op. cit.*

[12] M. ZABLOCKI *et al.*, « Intelligent video surveillance systems for public spaces – a survey », *Journal of Theoretical and Applied Computer Science*, 2014, p. 15.

[13] Elle est reconnue par la CNIL comme étant une application de la VSA, même si elle l'exclut par la suite de

8 Certains de ces usages sont envisagés dans le cadre de l'expérimentation de la VSA la surveillance des JO 2024. Notons néanmoins que le recours à la reconnaissance faciale et plus largement, aux systèmes d'identification biométrique, y a été explicitement exclu, dans la mesure où ils sont considérés comme plus attentatoires que d'autres applications de la VSA (voy. *infra* n° 35).

Section 2. Les avantages

9 Depuis plusieurs années, des études démontrent l'inefficacité de la vidéosurveillance par des caméras « classiques ». Peu, voire pas dissuasive, elle n'effraie ni les délinquants, ni les terroristes[14]. Son coût de déploiement et de maintenance est par ailleurs élevé[15].

10 Dans un tel contexte, la VSA est promue par l'industrie comme une solution révolutionnaire qui tiendra les promesses que sa prédécesseuse n'a pas su tenir. En effet, le visionnage des vidéos est une tâche chronophage pour la police, qui risque par ailleurs de manquer quelques détails sur les images. La promesse de la VSA est de remédier à ces problèmes. Grâce à la puissance de calcul à faible coût des machines[16], cette technologie permet d'automatiser l'exploitation des images captées par les caméras qui demandait jusqu'alors une intervention humaine, tout en offrant une analyse de certains paramètres plus précise que celle effectuée par un humain. La valorisation des parcs de caméras existants peut également être mentionnée, dans la mesure où la VSA est susceptible d'en faire usage plus efficace, qui justifierait ainsi son coût. La Commission nationale de l'informatique et des libertés (ci-après « la CNIL ») tempère néanmoins ces affirmations en appelant à ne pas céder au chant des sirènes du « solutionnisme technologique », lequel nous pousserait à considérer la VSA comme efficace par nature et à lui attribuer la capacité de résoudre de nombreux problèmes[17].

Section 3. Les risques

11 Le recours à la vidéosurveillance algorithmique n'est cependant pas sans risque. Fruit de l'association de l'intelligence artificielle et de la vidéosurveillance, la VSA intensifie la surveillance des citoyens (§1). Son caractère intrusif se confronte à un risque de dérives et de banalisation, dont les conséquences sur les droits fondamentaux sont graves (§2). À cela s'ajoutent un large potentiel d'adaptabilité à divers usages (§3) et des risques inhérents aux technologies d'IA (§4).

§1. Un risque accentué de surveillance et d'analyse généralisées

12 Comme le souligne la CNIL, la vidéosurveillance change fondamentalement de nature et d'échelle lorsqu'elle est associée à des traitements algorithmiques. De fait, dans le cadre de la vidéosurveillance « classique », seul un nombre restreint de personnes situées derrière un écran de contrôle visionnent ou enregistrent les images de personnes, qui se trouvent dans le champ de vision des caméras. De plus, ces images ne fournissent que les informations perçues par les personnes y ayant accès, lesquelles n'en visionnent d'ailleurs que rarement l'intégralité et plutôt de manière aléatoire ou à l'occasion d'une recherche ciblée[18].

---

son analyse ; CNIL, « Caméras dites 'intelligentes' ou 'augmentées' dans les espaces publics », disponible sur https://www.cnil.fr, 19 juillet 2022, p. 3.

[14] C. CHAZAL, « La vidéosurveillance est-elle efficace ? », *Le Monde*, 17 mai 2018 ; M. GILL et A. SPRIGGS, « *Assessing the impact of CCTV* », disponible sur https://techfak.uni-bielefeld.de, février 2005.

[15] COUR DES COMPTES, « Référé : Le plan de vidéoprotection de la préfecture de police de Paris », disponible sur https://www.ccomptes.fr, 10 février 2022, p. 1.

[16] M. ZABLOCKI *et al.*, *op. cit.*, p. 14.

[17] CNIL, « Caméras dites 'intelligentes'… », *op. cit.*, p. 7 à 9.

[18] CNIL, « Caméras dites 'intelligentes'… », *ibidem*, p. 9.

Si les informations obtenues par le biais de la vidéosurveillance « classique » sont donc relativement limitées, il en va autrement pour la VSA. Elle permet de s'affranchir de la limite matérielle que posait l'intervention humaine en confiant l'analyse des images aux machines dont la puissance de calcul et la rapidité ne sont plus à démontrer. L'analyse systématique et automatisée des images que permettent ces dernières élargit ainsi considérablement les informations qui pourraient en être déduites. De plus, l'enjeu n'est plus de filmer les personnes, mais de les analyser de manière automatisée, en traitant des volumes massifs de données à caractère personnel, afin d'inférer des informations qui pourraient être utilisées pour prendre des décisions ou des mesures concrètes les concernant[19]. 13

Ainsi, en ce que la VSA opère un changement d'échelle et de nature du traitement des données à caractère personnel des citoyens, elle se distingue de la vidéosurveillance classique. L'ampleur du traitement et son caractère plus intrusif emporte par ailleurs un risque d'atteintes comparativement plus graves aux droits fondamentaux et aux libertés des personnes concernées. Une telle remarque s'applique à plus forte raison lorsque ces dispositifs sont déployés dans les espaces publics, où de nombreuses libertés individuelles s'exercent[20]. 14

§2. Les dérives et la banalisation de technologies intrusives

Il n'est par ailleurs pas exclu qu'une fois les dispositifs de VSA installés, ces derniers soient utilisés à d'autres fins que celles qui justifiaient leur installation. Des dérives à l'égard d'outils de surveillance mis en place pour contrôler la pandémie du covid-19 ont déjà été observées dans plusieurs pays, dont la Chine[21], l'Australie[22] et les Etats-Unis[23]. Le danger est ici que la VSA soit détournée pour surveiller des mouvements de l'opposition politique, des militants, des journalistes et d'autres groupes jugés subversifs ou dangereux pour l'ordre public. Cela pourrait conduire à une atteinte à la liberté d'expression, à la liberté de la presse et à la liberté d'association[24]. 15

Parallèlement, certains s'inquiètent du risque de banalisation de ces technologies intrusives. En effet, normaliser la surveillance dans l'espace public peut conduire à accepter progressivement la surveillance dans d'autres domaines de la vie, tels que le lieu de travail, les écoles, des domiciles privés, voire les espaces en ligne[25]. Dans un contexte où la surveillance 16

[19] CNIL, « Caméras dites 'intelligentes'… », *ibidem*, p. 9.
[20] CNIL, « Caméras dites 'intelligentes'… », *ibidem*, p. 9.
[21] En Chine, par exemple, des QR codes de santé indiquant qu'une personne aurait contracté ou non la maladie du covid-19 ont été instrumentalisés pour empêcher des citoyens de manifester. Il s'agissait plus précisément d'un groupe de clients d'une banque, dont une partie du capital avait été gelée à la suite d'une enquête sur ses actionnaires. En juin 2022, ils se sont retrouvés bloqués lorsqu'ils ont tenté de se rendre à Zhengzhou pour protester contre l'impossibilité d'accéder à leurs comptes bancaires en ligne depuis plusieurs mois. Leurs QR codes avaient viré au rouge au moment de débarquer dans la ville ; voy G. BURKE *et al*., « Police seize on COVID-19 tech to expand global surveillance », disponible sur https://apnews.com, 21 décembre 2022.
[22] La police australienne a utilisé les données fournies par les utilisateurs des applications de *contact-tracing* durant la pandémie pour enquêter sur un meurtre, malgré la promesse que ces données ne seraient accessibles qu'au personnel chargé du *tracing* des contacts ; R. McGUIRK, « Police in Australia co-opted COVID-19 apps to fight crime », disponible sur https://apnews.com, 20 décembre 2022.
[23] Durant la pandémie, des agents fédéraux ont étudié la possibilité de croiser diverses des de santé, dont la toxicomanie et la santé mentale, pour des finalités qui dépassaient la gestion de la pandémie ; G. BURKE *et al*., *op. cit.*
[24] AMNESTY, Contribution extérieure dans l'affaire n°2023-850 DC, devant le Conseil constitutionnel, du 17 mai 2023.
[25] AMNESTY, Contribution extérieure dans l'affaire n°2023-850 DC, devant le Conseil constitutionnel, du 17 mai 2023 ; CNIL, « Caméras dites 'intelligentes'… », *op. cit.*, p. 9.

du citoyen s'intensifie, cela augmente le risque d'atteinte aux droits fondamentaux et en particulier, au droit à la vie privée.

§3.Le potentiel d'adaptabilité des usages

17 Les dispositifs de VSA jouissent en outre d'un grand potentiel d'adaptabilité à une multitude d'usages (voy. *supra* n° 8). Il est en effet techniquement possible, parfois même simplement en ajustant des paramètres, de changer les fonctionnalités du dispositif. Ce faisant, des caméras « augmentées » pourraient être initialement installées pour analyser la fréquentation d'un lieu et ensuite, être utilisées pour suivre la trajectoire et les déplacements des individus. Une fois les caméras installées, il pourrait donc être relativement aisé pour les autorités d'ajouter certaines fonctionnalités qui n'avaient pas encore été envisagées[26].

18 De plus, la réaffectation du dispositif à d'autres usages est invisible. Une personne présente dans l'espace public n'y voit que des caméras. Rien ne lui indique qu'il s'agit désormais de caméras intelligentes capables, par exemple, de reconnaissance biométrique. Sauf à considérer que le changement de fonctionnalités ait fait l'objet de mesures de publicité, la personne n'a pas de moyen d'avoir conscience que ces caméras l'analysent, ni de quelle manière et sur base de quels critères. *A fortiori*, elle ne peut pas non plus protester contre le déploiement de « nouvelles » fonctionnalités[27]. À la lumière d'une enquête réalisée par le Défenseur des droits en France, il est par ailleurs fort probable qu'un citoyen lambda ne s'imagine même pas les fonctionnalités se cachant derrière ces caméras intelligentes. Cette étude démontre en effet qu'à peine plus d'un tiers des Français se sent bien informé sur le fonctionnement ou les domaines dans lesquels interviennent les technologies biométriques, dont de nombreuses applications relèvent de la vidéosurveillance algorithmique. Les Français seraient donc au courant de leur existence, mais ne semblent pas en maîtriser les usages[28].

19 Or, cette facilité à glisser silencieusement d'une fonctionnalité à l'autre est susceptible d'abus, à laquelle s'ajoutent les dérives liées à leur détournement évoquées ci-avant (voy. *supra* n^{os} 15 et s.). Une fois le dispositif de vidéosurveillance mis en place, le coût pour les autorités d'ajouter des fonctionnalités plus intrusives est en effet très faible, tant sur le plan technique que social.

§4.Les risques liés aux technologies d'IA

20 La VSA est une technologie reposant sur l'IA (voy. *supra* n°6). Elle hérite donc de certains de ses défauts, rassemblés ici sous trois thématiques différentes : la discrimination (A), la transparence (B) et la sécurité (C).

A. Entre biais et discrimination

21 Plusieurs études démontrent que les systèmes d'IA contiennent des biais[29]. L'existence de biais rend ces systèmes moins fiables et peut les conduire à produire des résultats discriminatoires. De fait, dans le cadre de la VSA, par exemple, lorsqu'un dispositif détecte un évènement « anormal », il le signale aux autorités qui prennent les mesures qui s'imposent, comme des amendes ou des arrestations administratives. Or, si le système classifie erronément l'évènement systématiquement parce qu'il est biaisé, cela peut entraîner des conséquences négatives sur les

[26] CNIL, « Caméras dites 'intelligentes'… », *ibidem*, p. 9.
[27] CNIL, « Caméras dites 'intelligentes'… », *ibidem*, p. 9.
[28] DÉFENSEUR DES DROITS, « Perception du développement des technologies biométriques en France : entre manque d'information et demande d'encadrement », disponible sur https://www.defenseurdesdroits.fr, 6 octobre 2022, p. 4.
[29] Voy. not. S. BAROCAS et A. SELBST, « Big Data's Disparate Impact », *California Law Review*, 2016, p. 671 à 732.

catégories de personnes qui ont davantage tendance à adopter le comportement identifié comme un évènement anormal. Comparativement, elles feront, en effet, plus que les autres l'objet des mesures – le cas échéant, répressives – ordonnées par les autorités.

Selon la doctrine, les biais peuvent intervenir tant au stade de l'entraînement du système d'IA, qu'à celui de la définition du problème et des variables employées par ce dernier. 22

D'abord, pour fournir le résultat souhaité, l'IA doit être entraînée sur un jeu de données. Or, ces données sont souvent biaisées. À cet égard, trois sources de biais peuvent être identifiées. La première est l'intervention humaine dans la sélection de l'échantillon de données, voire leur étiquetage s'il s'agit d'un apprentissage automatique supervisé. La deuxième est la sous-représentation de certains groupes de la population dans les données, ce qui peut réduire la précision des résultats les concernant et impacter le système dans son ensemble[30]. La troisième a trait à la problématique des biais historiques. Les données collectées et fournies au système sont le reflet de notre société et de ses inégalités. Dès lors, lorsque celles-ci sont utilisées, les IA tendent à reproduire les biais qu'elles contiennent dans leurs résultats et risquent ainsi de perpétuer certaines discriminations existantes[31]. La reconnaissance faciale, que la VSA rend possible à grande échelle, permet d'illustrer ce qui précède. Dans certaines études, les visages des femmes noires ont été identifiés à tort plus souvent que ceux des hommes blancs. Ces erreurs ont été attribuées à des biais dans la constitution des ensembles de données[32]. 23

Ensuite, lors du développement de l'algorithme, le programmeur doit définir le problème et ses variables. Il doit par conséquent effectuer des choix pour créer un modèle représentant le problème. Le modèle réduit nécessairement la réalité, car il ne peut inclure autant de variables que le monde réel. Or, selon la formulation du problème, où certaines variables seront inclues ou non, les différents groupes concernés seront affectés différemment[33]. En outre, le programmeur doit aussi choisir des variables qui lui semblent pertinentes. Dans le cas de la VSA telle qu'étudiée présentement, le problème que l'IA doit résoudre est généralement celui d'identifier des événements « anormaux » dans les espaces publics (voy. *supra* n°7). Il faudra donc définir ce qu'est un évènement anormal. Cette définition, et *a fortiori* l'algorithme, varieront selon la conception que s'en fait un programmeur et/ou selon celle qui lui est imposée par le cahier des charges. Or, les conséquences pratiques du choix de la définition sont importantes, puisque l'algorithme recommandera aux autorités d'intervenir ou non, ce qui pourrait mener dans certains cas à des arrestations. 24

Si définir correctement le problème est impératif, la tâche n'est pourtant pas aisée. De fait, les questions auxquelles il faut répondre sont particulièrement complexes : qu'est-ce qui est normal dans l'espace public et comment le traduire pour une machine ? À titre illustratif, en 2020, une expérimentation a été menée dans la station de métro des Halles à Paris pour repérer des comportements anormaux. Concrètement, un système avait été mis en place pour identifier les personnes statiques pendant plus de 300 secondes. Dans un tel contexte, un comportement 25

---

[30] M. CHORAŚ, *et al.*, « Machine Learning – The Results Are Not the only Thing that Matters! What About Security, Explainability and Fairness? », *Computational Science – ICCS*, V. Krzhizhanovskaya *et al.* (dir.), Cham, Springer, 2020, p. 620 et 621.

[31] M. MANN et T. MATZNER, « Challenging algorithmic profiling: The limits of data protection and anti-discrimination in responding to emergent discrimination », *Big Data & Society*, 2019, p. 2; S. BROWNE, *Dark Matters: On the Surveillance of Blackness*, Durham, Duke University Press, 2015, p. 89 à 131.

[32] Voy. not. J. BUOLAMWINI et T. GEBRU, « Proceedings of the 1st Conference on Fairness, Accountability and Transparency », *P.M.L.R.*, 2018, p. 77 à 91 ; J. CHARPENET et C. LEQUESNE ROTH, « Discrimination et biais genrés, Les lacunes juridiques de l'audit algorithmique », *Recueil Dalloz*, 2019, p. 1852.

[33] S. BAROCAS et A. SELBST, *op. cit.*, p. 677 à 692.

anormal était donc celui d'une personne statique[34]. Pourtant, cette définition emporte des conséquences concrètes pour les personnes qui ne considèrent pas l'espace public comme un lieu de passage[35]. Selon cette conception de l'anormalité, les sans-abris ou encore les artistes de rue seraient systématiquement épinglés par le système comme ayant des comportements anormaux, ce qui pourrait être stigmatisant. Au-delà de la traduction de la normalité en variables qu'une machine peut comprendre, il existe également un risque de stigmatisation et de discrimination des personnes présentant un trouble du spectre autistique. En effet, pour ces dernières, les codes de la société n'ont rien d'une évidence. Elles risquent donc d'adopter des comportements « anormaux »[36].

B. La transparence et le contrôle

26 Au-delà de la question des biais, les systèmes d'IA souffrent actuellement d'un problème d'opacité qui rendent ces derniers invisibles, tant sur le plan technique que le plan juridique. Certaines techniques d'apprentissage automatique tendent en effet à produire des systèmes d'IA dont il est pratiquement impossible de comprendre complètement le raisonnement et les décisions[37]. Dans le cadre de la VSA, cela signifie qu'il est pratiquement impossible de retracer les corrélations entre les données traitées et le résultat produit, un signalement d'attention par exemple. Cette opacité technique se double d'une opacité juridique, causée par le refus des entreprises de communiquer les éléments techniques de leur système en se fondant sur les secrets d'affaires et la propriété intellectuelle[38]. Or, la transparence est essentielle à l'action, la dignité[39] et le contrôle humains[40]. Il est en effet important que les utilisateurs d'un système d'IA comprennent comment il fonctionne pour évaluer de manière critique le résultat et éviter de suivre aveuglément les recommandations de la machine. De même, les utilisateurs doivent pouvoir justifier cette décision auprès des personnes concernées par cette dernière. Cela est particulièrement essentiel pour les autorités publiques, qui en sont utilisatrices, sous peine de perdre la confiance des citoyens[41].

27 Outre le manque de transparence, il existe un risque que les utilisateurs deviennent dépendants des systèmes d'IA et les emploient sans examiner d'un œil critique les résultats produits. Entre la fatigue, l'ennui et le manque de temps[42], de nombreux facteurs impactent la capacité d'un humain à garder le contrôle sur ces systèmes.

C. Les risques liés à la sécurité et à la protection des données

28 Le déploiement de la VSA dans les espaces publics soulève des préoccupations en matière de sécurité et de fiabilité. La VSA doit en effet reposer sur (i) un réseau de caméras fiable, (ii) une IA de traitement d'images robuste, à savoir qu'elle doit être capable de fonctionner de

---

[34] INSTITUT PARIS RÉGION, « La sécurité à l'heure de l'intelligence artificielle », disponible sur https://www.institutparisregion.fr, 6 février 2020, p. 2 et 4.
[35] LA QUADRATURE DU NET, *Projet de loi relatif aux Jeux Olympiques et Paralympiques de 2024 : dossier d'analyse de la vidéosurveillance automatisée*, 21 janvier 2023, p. 30.
[36] Voy. not. O. KEYES, « Automating autism: Disability, discourse, and Artificial Intelligence », *Journal of Sociotechnical Critique*, 2020, p. 1-31.
[37] . F. DESCHESNE *et al*., « AI & Ethics at the Police: Towards Responsible use of Artificial Intelligence in the Dutch Police », disponible sur https://scholarlypublications.universiteitleiden.nl, mars 2019, p. 3.
[38] C. LEQUESNE ROTH et J. KELLER, *op. cit.*, p. 63.
[39] Le droit à la dignité humaine est lié au respect de l'autonomie humaine ; GROUPE D'EXPERTS INDÉPENDANTS DE HAUT NIVEAU SUR L'INTELLIGENCE ARTIFICIELLE, *Lignes directrices en matière d'éthique pour une IA digne de confiance*, 2019, p. 14.
[40] GROUPE D'EXPERTS INDÉPENDANTS DE HAUT NIVEAU SUR L'INTELLIGENCE ARTIFICIELLE, *ibidem*, p. 19.
[41] F. DESCHESNE *et al*., *op. cit*., p. 6.
[42] F. DESCHESNE *et al*., *ibidem*, p. 20.

manière fiable et précise, même en présence de diverses incertitudes, perturbations ou tentatives de contournement, et (iii) une base de données sécurisée, dont les utilisateurs ne perdent pas la maîtrise.

29 Premièrement, lorsque ces systèmes ont recours à des équipements incapables de capturer des images de qualité optimale, les résultats obtenus deviennent incertains. Ce manque de fiabilité menace tant les individus ciblés que la sécurité publique dans son ensemble[43]. D'une part, le risque est de cibler injustement des personnes en raison de la qualité médiocre des images, ce qui peut entraîner des conséquences graves (voy. *supra* n°). À titre illustratif, dans le cadre de l'expérimentation dans la station de métro des Halles évoquées plus haut (voy. *supra* n°), la mauvaise qualité des images fournies par les caméras aurait causé nombreux faux positifs, c'est-à-dire qu'un évènement était identifié à tort comme anormal. La qualité médiocre des images était attribuée non seulement à l'ancienneté du parc de caméras, qui ne fournissait que des images à faible résolution, mais également à des angles de vue difficiles[44]. D'autre part, face à des occurrences trop nombreuses de faux positifs ou de faux négatifs, où les systèmes n'identifient pas des évènements anormaux alors qu'ils auraient dû, les autorités ou entités ayant recours à de tels systèmes risquent de voir la confiance placée dans ces derniers faiblir, ce qui pourrait diminuer l'efficacité des forces humaines chargées de leur utilisation.

30 Deuxièmement, les systèmes d'IA peuvent être contournés et manipulés. Des études ont démontré que l'IA est fondamentalement vulnérable à certains types d'attaques[45], dont celles d'évasion. Ces dernières visent à fournir des exemples adverses à l'IA afin d'éviter qu'elle fonctionne correctement. Il suffit d'altérer légèrement les données fournies à la machine afin de l'induire en erreur[46]. Dans le cas de la reconnaissance faciale, par exemple, il a été démontré que l'ajustement de quelques pixels au coin de l'œil d'une personne[47] ou encore l'ajout d'autocollants en papier à un chapeau[48] suffisaient à rendre le système inefficace.

31 Troisièmement, les bases de données sur lesquelles se fondent ces technologies pourraient être compromises et échapper au contrôle des autorités ou entités qui ont recours à la VSA. À cet égard, rappelons que les caméras connectées qui composent les systèmes de VSA constituent des points d'entrée potentiels pour des attaques informatiques. Les conséquences de telles attaques sont potentiellement graves et peuvent affecter tant les autorités ou les entités qui utilisent ces dispositifs que les personnes dont les données y figurent. Des vols de données biométriques, considérées comme des données à caractère personnel « sensibles » et dont le traitement est possible par la VSA (voy. *infra* n^{os} 54 et 55), ont déjà eu lieu. L'affaire Clearview AI en est un exemple éloquent. En 2020, la base de données de la société américaine du même nom, constituée à partir de milliards de données biométriques collectées sur les médias sociaux, a connu une importante faille de sécurité. Son code source ainsi que certaines clés privées sont devenues accessibles au public, permettant à quiconque d'accéder aux données. Les conséquences d'une faille de sécurité, particulièrement lorsqu'il s'agit de données sensibles, sont graves car il est difficile de les corriger[49]. S'agissant des données biométriques, outre une

---

[43] C. LEQUESNE ROTH et J. KELLER, *op. cit.*, p. 38.
[44] INSTITUT PARIS RÉGION, *op. cit.*, p. 2.
[45] Voy. not. T. ANASTASIOU *et al.*, « Towards Robustifying Image Classifiers against the Perils of Adversarial Attacks on Artificial Intelligence Systems », *Sensors*, 2022, p. 2 à 22.
[46] A. LO LUCA, « Adversarial Machine Learning: Attacks and Possible Defense Strategies », disponible sur https://towardsdatascience.com, 1er août 2021.
[47] A. J. BOSE et P. AARABI, « Adversarial Attacks on Face Detectors using Neural Net based Constrained Optimization », *arXiv*, 2018, p. 2.
[48] S. KOMKOV et A. PETIUSHKO, « AdvHat: Real-world adversarial attack on ArcFace Face ID system », *arXiv*, 2019, p. 1 à 9.
[49] CNIL, « Reconnaissance faciale : pour un débat à la hauteur des enjeux », disponible sur https://www.cnil.fr,

atteinte importante à la vie privée des personnes concernées, ces dernières risquent de subir une usurpation d'identité, contre laquelle il sera difficile de lutter. En effet, elles ne peuvent pas modifier leurs données biométriques comme elles le pourraient avec un simple mot de passe[50].

Chapitre 2. Un cas d'étude : l'expérimentation de la VSA pour les JO 2024

32 En dépit des risques identifiés ci-dessus, le gouvernement français a décidé d'expérimenter la VSA dans le cadre de la surveillance des JO 2024 ». Dans un « Livre blanc de la sécurité intérieure, le ministère français de l'Intérieur évoque déjà l'expérimentation de nouvelles technologies à des fins sécuritaires, avec l'objectif assumé de renforcer la sécurité aux JO 2024[51]. Ce plan d'action est ensuite précisé dans un rapport annexe à la « Loi d'orientation et de programmation du ministère du l'Intérieur »[52]. De policiers « augmentés » au moyen d'exosquelettes de protection au brouillage de drones malveillants, un arsenal de haute technologie est envisagé, avec ses besoins de financement et son encadrement législatif. Parmi ces outils, figure la « vidéoprotection intelligente » [53] ou « vidéosurveillance intelligente », selon que l'accent soit mis sur la sécurité ou le respect de la vie privée.

33 La volonté d'expérimentation d'une telle technologie se concrétise au dépôt du projet de loi relatif aux JO 2024 et portant diverses autres dispositions, déposé au Sénat français le 22 décembre 2022 en procédure accélérée. Ce dernier contient en effet l'article 7, qui vise à autoriser, à titre expérimental, « l'utilisation de traitements algorithmiques permettant d'identifier, sur les images captées par des dispositifs de vidéoprotection, des évènements révélant un risque pour la sécurité des personnes. »[54] Le 12 avril 2022, le texte de loi est adopté. L'article 7 devient l'article 10.

34 L'article 10 autorise l'expérimentation de la VSA jusqu'au 31 mars 2025, avec pour seule et unique objectif d'assurer la sécurité de manifestations sportives, récréatives ou culturelles qui sont particulièrement exposées à des risques d'actes de terrorisme ou d'atteinte à la sécurité des personnes.

35 Plus concrètement, il s'agit de permettre de détecter, en temps réel, grâce à un réseau de caméras fixes et des caméras mobiles, équipées sur des drones, 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 différents services déployés, comme la police, les pompiers, etc. En particulier, le dispositif signalerait « des évènements anormaux, des mouvements de foule, des objets abandonnés ou des situations présumant la commission d'infractions » et permettra d'effectuer des analyses statistiques, en analysant par exemple le flux de fréquentation[55]. Le traitement de données biométriques est interdit et avec lui, le recours à des

---

14 novembre 2019, p. 10.

[50] D. RYJOUKHINA, « Les données biométriques et l'identité — Quelle protection juridique pour ces données à caractère personnel ? », *R.D.T.I.*, 2018, p. 12.

[51] MINISTÈRE DE L'INTÉRIEUR, « Livre blanc de la sécurité intérieure », disponible sur https://www.interieur.gouv.fr, 16 novembre 2020, p. 159 et 160.

[52] L. n°2023-22, 24 janvier 2023, d'orientation et de programmation du ministère de l'intérieur (« LOPMI »), NOR : IOMD2223411L ; Projet de loi d'orientation et de programmation du ministère de l'intérieur, Rapport annexé, Sén., 2022-2023, n°876, NOR : INTD2204555L/Bleue-1.

[53] Projet de loi relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions, *J.O.R.F.*, Sén., 2022-2023, n°220, art. 7, I.

[54] Projet de loi relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions, exposé des motifs, *J.O.R.F.*, Sén., 2022-2023, n°220, p. 5 et 6.

[55] Projet de loi relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions, étude d'impact, *J.O.R.F.*, Sén., 2022-2023, n°220, p. 107.

technologies de reconnaissance faciale[56]. La loi française prend ici une définition plus restreinte de la VSA.

L'autorisation de l'expérimentation de la VSA s'accompagne de plusieurs garanties. Outre l'interdiction de traitement de données biométriques, les traitements automatisés ne peuvent procéder à aucune interconnexion ni à aucune mise en relation automatisée avec d'autres traitements de données à caractère personnel. Le dispositif ne peut par ailleurs procéder qu'à un signalement d'attention par rapport à évènement déterminé et ne fonde pas de décision individuelle ou de poursuites. Il doit également remplir certaines exigences en matière de cybersécurité[57]. Au surplus, le public est préalablement informé du recours à des traitements algorithmiques[58]. Enfin, une analyse d'impact sera menée au moment d'autoriser le système de VSA développé par une entreprise[59]. 36

Titre II. L'ENCADREMENT (LACUNAIRE) DE LA VSA PAR LE DROIT DE LA PROTECTION DES DONNÉES

À la lumière des risques posés par le déploiement des technologies de VSA et de leur popularité grandissante auprès des services publics de l'Union européenne[60], il est impératif d'examiner leur conformité avec les normes juridiques établies au niveau européen. La législation actuelle en matière de protection des données à caractère personnel nous semble la plus aboutie en l'état pour encadrer la mise en place de la VSA, bien qu'elle se révèle lacunaire, voire technologiquement dépassée sur certains aspects. Ce corpus juridique est constitué de la Charte des droits fondamentaux de l'Union européenne et en particulier de son article 8, consacrant un droit fondamental à la protection des données personnel (Section 1), ainsi que du RGPD et de la directive police-justice (Section 2). 37

Notons qu'en raison du large éventail d'applications possibles auxquelles peuvent être destinés les dispositifs de VSA, appelant chacun leurs commentaires, et afin d'éviter une analyse trop superficielle, nous faisons le choix d'examiner à titre principal la conformité du dispositif de VSA envisagé par le gouvernement français décrit ci-avant (voy. *supra* n^{os} 32 et s.). 38

Chapitre 1. Le droit primaire de l'UE : la Charte des droits fondamentaux de l'UE

L'article 8 de la Charte consacre un droit fondamental à la protection des données personnel et s'applique à des dispositions légales servant de base juridique à un traitement de données à caractère personnel (Section 1). Un traitement de données à caractère personnel constituant une ingérence dans ce droit, il doit respecter les conditions prévues à l'article 52, paragraphe 1er, de la Charte, pour être licite (Section 2). 39

Section 1. L'applicabilité de l'article 8 de la Charte

Les dispositions de la Charte s'adressent aux États membres lorsqu'ils mettent en œuvre le droit de l'Union[61]. C'est notamment le cas lorsque des dispositions nationales se fondent sur une dérogation prévue par le droit de l'UE ou lorsqu'elles affectent directement une matière 40

[56] L. n°2023-380, 19 mai 2023, précitée, art. 10, IV.
[57] L. n°2023-380, 19 mai 2023, précitée, art. 10, VI. al. 1
[58] L. n°2023-380, 19 mai 2023, précitée, art. 10, III.
[59] L. n°2023-380, 19 mai 2023, précitée, art. 10, V, al. 3 et VII, al. 2.
[60] Voy. à cet égard l'étude suivante : C. LEQUESNE ROTH, « New Surveillance Technologies in Public Spaces Challenges and Perspectives for European Law at the Example of Facial Recognition », disponible sur https://www.academia.edu, avril 2021, p. 1 à 96.
[61] Art. 51, §1, de la Charte.

régie par ce dernier[62]. Une loi portant sur la VSA ou visant à la déployer relève de la Charte. En effet, en ce que la VSA consiste en la collecte et l'analyse de séquences vidéo de personnes physiques, elle implique des traitements de données à caractère personnel, lesquels sont régis par des instruments de droit de l'Union (Chapitre 2).

41 En outre, une disposition législative qui, à l'instar de l'article 10 de la loi relative aux JO 2024, sert de base juridique au traitement de données à caractère personnel par VSA interfère directement avec les droits garantis par les articles 7 et 8 de la Charte. L'objet de la présente étude étant d'examiner la légalité de la VSA au regard du droit de la protection des données, seul l'article 8 sera analysé. De fait, si l'article 7 reconnait un droit à la vie privée, c'est l'article 8 de la Charte qui consacre un droit fondamental à la protection des données à caractère personnel. Ce dernier soumet leur traitement à certaines conditions, qui seront développées au moment d'adresser le droit dérivé de l'UE en matière de protection des données à caractère personnel auquel est soumis la VSA (Chapitre 2). Pour l'instant, notons que ces données doivent être traitées de manière loyale, à des fins déterminées et avec le consentement de la personne concernée, ou sur la base d'un autre fondement légal légitime prévu par la loi. La Charte précise également que « [t]oute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification ».[63]

Section 2. La VSA comme limitation à l'article 8 de la Charte

42 Le droit à la protection des données à caractère personnel consacré à l'article 8 de la Charte n'est pas absolu. Conformément à l'article 52, paragraphe 1er, de la Charte, il peut faire l'objet de limitations, moyennant le respect de certaines exigences. Ces limitations doivent être prévues par la loi (§1) et respecter le contenu essentiel du droit à la protection des données à caractère personnel (§2). Elles doivent également répondre effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui (§3) et être proportionnées (§4).

43 À titre liminaire, il convient de souligner que tout traitement de données à caractère personnel constitue une ingérence dans ce droit. Pour être considérée comme licite, cette ingérence doit remplir les conditions énoncées ci-dessus, peu importe que les données traitées concernent la vie privée d'une personne, soient de nature sensible ou que les personnes concernées en aient subi des effets négatifs.[64]

§1. La légalité

44 L'article 52, paragraphe 1er, de la Charte exige que la limitation soit prévue par la loi. Cette exigence impose non seulement que l'ingérence trouve son fondement en droit interne, mais elle vise aussi la qualité de cette loi. Celle-ci doit être suffisamment claire dans ses termes pour donner aux citoyens une indication adéquate des conditions et des circonstances dans lesquelles les autorités ont le droit de recourir à des mesures de surveillance et de collecte de données[65]. Elle doit contenir les éléments essentiels du traitement ainsi que prévoir des garanties

---

[62] X, « Partie III — Champ d'application, interprétation et effets de la charte », disponible sur https://e-justice.europa.eu, 25 novembre 2020.
[63] Art. 8, §2, de la Charte.
[64] A.D.F., *Manuel de droit européen en matière de protection des données*, Luxembourg, Office des publications de l'Union européenne, 2018, p. 48 et 49.
[65] Cour eur. D.H., arrêt *Shimovolos c. Russia*, 21 juin 2011, §68.

suffisantes pour assurer le respect du droit en question[66]. Le but est de protéger le citoyen contre d'éventuelles atteintes arbitraires par le pouvoir exécutif[67].

45 En fonction des différentes applications de la VSA, des données à caractère personnel sensibles pourraient être traitées, en particulier des données biométriques (voy. *infra* n^{os} 78 à 98). Dès lors, une loi spécifique décrivant précisément l'application et les conditions de son utilisation aurait été souhaitable. Dans le cadre de l'expérimentation envisagée par le gouvernement français pour les JO 2024, il est donc regrettable que la VSA, au regard de son caractère fort attentatoire aux droits et libertés des citoyens, ait été autorisée par une loi fourre-tout relative aux JO, déléguant la détermination d'éléments essentiels[68] du traitement au pouvoir exécutif[69]. La loi relative aux JO 2024 fournit néanmoins certaines garanties comme un déploiement expérimental de la technologie, limité dans le temps et l'espace, ainsi qu'un encadrement précis du développement de la technologie qui sera utilisée[70]. L'absence de traitement de données biométriques est également présentée comme une garantie par la loi[71], mais cette affirmation est non seulement contestable, mais aussi contestée (voy. *infra* n^{os} 78 à 98).

§2.L'essence du droit à la protection des données à caractère personnel

46 L'examen du respect de « l'essence du droit » est un test préalable à la mise en balance entre les considérations qui ont présidé à l'adoption de la mesure constituant une ingérence et son caractère proportionné (voy. *infra* n° 50). De fait, une atteinte au contenu essentiel d'un droit fondamental rend *per se* la limitation à ce dernier contraire à la Charte, indépendamment de toute considération liée à la nécessité ou aux garanties qui auraient été fournies. Une telle atteinte intervient lorsqu'une mesure impose une limitation à l'exercice d'un droit fondamental qui est telle, en termes d'intensité et de portée, qu'elle remet en cause ce droit[72].

47 L'affaire *Schrems*[73] en est une bonne illustration. La Cour de justice de l'UE (ci-après « la CJUE ») y a, pour la première fois, déclaré invalide une mesure de l'UE au motif qu'elle ne respectait pas l'essence de deux droits fondamentaux : le droit au respect de la vie privée et le droit à une protection juridictionnelle effective. L'affaire concernait l'accord *Safe Harbor*, visant à faciliter les transferts de données à caractère personnel entre l'UE et les États-Unis en garantissant un niveau adéquat de protection des données. Les limitations au droit au respect de la vie privée des personnes concernées étaient particulièrement étendues, si bien qu'il n'existait en réalité plus de vie privée. Les autorités américaines pouvaient en effet avoir un accès illimité au contenu de toutes les données à caractère personnel transférées de l'UE vers les États-Unis[74].

---

[66] Cour eur. D.H., arrêt *Rotaru c. Roumanie*, 4 mai 2000, §57 et 59.

[67]Voy. en ce sens, C.J., arrêt *WebMindLicenses c. Nemzeti Adó- és Vámhivatal Kiemelt Adó- és Vám Főigazgatóság*, 17 décembre 2015, C-419/14, EU:C:2015:832, point 81 ; Cour. eur. D.H., arrêt *Malone c. Royaume-Uni*, 2 août 1984, §67 ;Cour eur. D.H., arrêt *Gillan et Quinton c. Royaume-Uni*, 12 janvier 2010, §77.

[68] Il s'agit en autres des événements prédéterminés que le traitement a pour objet de signaler et des conditions d'habilitation et de formation des agents pouvant accéder aux signalements du traitement. Ces aspects auraient pu être intéressants à discuter au sein d'une assemblée démocratiquement élue ; L. n°2023-380, 19 mai 2023, précitée, art. 10, V, al. 2.

[69] L. n°2023-380, 19 mai 2023, précitée, art. 10, V.

[70] L. n°2023-380, 19 mai 2023, précitée, art. 10, I et VI à VIII.

[71] L. n°2023-380, 19 mai 2023, précitée, art. 10, IV.

[72] K. LENAERTS, « Limits on Limitations: The Essence of Fundamental Rights in the EU », *German Law Journal*, 2019, p. 782 et 784.

[73] C.J., arrêt *Schrems v. Data Protection Commissioner*, 8 octobre 2015, C-362/14, EU:C:2015:650.

[74] K. LENAERTS, *op. cit.*, p. 779.

48 Dans le cadre d'un recours contre la loi relative aux JO 2024 devant le Conseil constitutionnel français, la société civile a déposé une contribution argumentant que la VSA telle qu'elle était envisagée portait atteinte au contenu essentiel des articles 7, 8 et 11 de la Charte, touchant respectivement au droit à la vie privée, au droit à la protection des données à caractère personnel et à la liberté d'expression. Selon elle, le contenu essentiel de ces droits comprend un droit à ne pas faire l'objet « d'une surveillance constante et généralisée dans l'espace public »[75]. Si dans sa décision, le Conseil constitutionnel n'adresse pas explicitement cet argument, il souligne néanmoins toutes les garanties que le législateur a assorties au dispositif[76]. Cette approche fait écho à la jurisprudence la CJUE. Dans l'affaire *Digital Rights Ireland*, la Cour a estimé que l'essence du droit à la protection des données à caractère personnel avait été respectée parce que la limitation était encadrée par certains principes de protection et de sécurité des données imposant l'adoption de mesures techniques et organisationnelles garantissant notamment un accès limité aux données[77]. L'existence d'un dispositif de VSA ne porte donc pas nécessairement atteinte à l'essence du droit à la protection des données à caractère personnel pour autant que ce dernier soit encadré et limité. C'est le cas du dispositif autorisé par l'article 10 de la loi. Il ne s'agit ainsi pas pour l'instant d'une surveillance constante et généralisée de l'espace public. Un objectif légitime

49 La condition la moins contentieuse de l'article 52, paragraphe 1er de la Charte, est sans doute la légitimité de l'objectif poursuivi, lequel doit être considéré comme un objectif d'intérêt général reconnu par l'Union. Tel est notamment le cas de la sécurité publique[78], invoquée depuis les années 90 pour justifier la mise en place de caméras dans l'espace public[79]. L'article 10, paragraphe I, de la loi relative aux JO 2024 la reconnaît d'ailleurs comme objectif aux côtés de la lutte contre de potentiels actes terroristes.

§3.La nécessité et la proportionnalité

50 Un objectif d'intérêt général – aussi fondamental soit-il – ne justifie pas, en soi, une limitation à un droit fondamental[80]. La mesure doit être appropriée pour atteindre ce dernier et ne doit pas dépasser les limites de ce qui est approprié et nécessaire pour ce faire[81]. Cette appréciation dépendant entre autres de la nature des données traitées et, notamment, de leur qualification en tant que données biométriques, nous renvoyons aux développements ci-après relatifs à l'examen de la nécessité et la proportionnalité sous le RGPD et la directive police-justice (voy. *infra* nos 104 et s.).

Chapitre 2. Le droit dérivé de l'UE : le RGPD et la directive police-justice

51 Le RGPD et la directive police-justice sont des instruments destinés à mettre en œuvre l'article 8 de la Charte. Dès lors que la VSA implique divers traitements de données à caractère personnel, l'un ou l'autre trouveront à s'appliquer selon qu'elle soit employée ou non dans un

---

[75] LA QUADRATURE DU NET, Contribution extérieure dans l'affaire n°2023-850, devant le Conseil constitutionnel, du 17 mai 2023.
[76] Conseil constitutionnel, 17 mai 2023, n°2023-850 DC, points 26 à 49.
[77] C.J. (gde ch.), arrêt *Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources et Kärntner Landesregierung*, 8 avril 2014, aff. jointes C-293/12 et C-594/12, EU:C:2014:238, point 40.
[78] Voy. not, C.J. (gde ch.), arrêt *Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources et Kärntner Landesregierung*, 8 avril 2014, aff. jointes C-293/12 et C-594/12, EU:C:2014:238, points 41 à 44.
[79] X, « Hauts-de-Seine les caméras espionnes de Levallois : Le système de vidéo-surveillance installé par le maire suscite des protestations », *Le Monde*, 14 mars 1993.
[80] C.J. (gde ch.), arrêt *Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources et Kärntner Landesregierung*, 8 avril 2014, aff. jointes C-293/12 et C-594/12, EU:C:2014:238, point 51.
[81] C.J. (gde ch.), arrêt *Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources et Kärntner Landesregierung*, 8 avril 2014, aff. jointes C-293/12 et C-594/12, EU:C:2014:238, point 46.

contexte répressif (Section 1). Ce faisant, la VSA est soumise aux garanties prévues dans ces instruments (Section 2). Certains argumentent également que la VSA, lorsqu'elle traite des données à caractère personnel, procède également – et nécessairement – au traitement de données biométriques, pour lequel un régime spécifique existe sous le RGPD et la directive. Dès lors, il convient d'examiner si de telles allégations sont fondées ainsi que le régime qui serait applicable, le cas échéant (Section 3).

Section 1. L'applicabilité du RGPD et de la directive police-justice

52 Compte tenu des finalités de mise en œuvre des dispositifs de VSA mis en place à titre expérimental pour les JO 2024, ces derniers sont soumis au respect du RGPD et de la directive police-justice[82], à l'exception de ceux mis en œuvre à des fins de « sauvegarde des installations utiles à la défense nationale » ou de « prévention d'actes de terrorisme »[83]. Ces deux instruments composent le « paquet européen relatif à la protection des données à caractère personnel ». Leurs champs d'application sont distincts, mais se veulent complémentaires. Ainsi, le RGPD s'applique de manière générale en matière de protection des données à caractère personnel, à l'exception des traitements mis en œuvre pour l'exercice d'activités qui ne relèvent pas du champ d'application du droit de l'Union européenne. À ce titre, la CNIL souligne que les activités de sûreté de l'Etat ou de défense nationale ne sont pas soumise au RGPD[84], mais à la loi française « Informatique et Libertés »[85]. Le RGPD ne couvre pas non plus les traitements relevant de la *lex specialis* que constitue la directive police-justice. Celle-ci s'applique au traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces[86].

53 L'application du RGPD et de la directive police-justice[87], requiert l'existence d'un traitement de données à caractère personnel. Notons que ces deux instruments partagent un même univers terminologique. Ce faisant, les notions de « données à caractère personnel » et de « traitement » ont la même portée dans l'un et l'autre.

54 Les données à caractère personnel recouvrent « toute information se rapportant à une personne physique identifiée ou identifiable »[88]. À cet égard, est réputée identifiable « une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, […], ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale »[89]. Sauf à considérer que l'espace surveillé ne sera jamais pénétré par une personne physique, la vidéosurveillance entraîne la collecte et la conservation d'images ou d'informations sur toutes les personnes entrant dans ce dernier. Les personnes sont identifiables sur la base de leur

[82] Projet de loi relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions, Avis du Conseil d'Etat, *J.O.R.F.*, Sén., 2022-2023, n°220, p. 5.
[83] CNIL, « Vidéoprotection : quelles sont les dispositions applicables ? », disponible sur https://www.cnil.fr, 13 décembre 2019.
[84] CNIL, « Directive 'Police-Justice': de quoi parle-t-on ? », disponible sur https://www.cnil.fr, 20 février 2019.
[85] L. n° 78-17, 6 janvier 1978, relative à l'informatique, aux fichiers et aux libertés (« LIL »).
[86] Art. 1er, §1er de la Directive police-justice.
[87] Pour être exact, il s'agit des législations nationales la transposant. En France, il s'agit de la loi relative à l'informatique, aux fichiers et aux libertés : précitée. L. n° 78-17, 6 janvier 1978, précitée.
[88] Art. 4, 1), du RGPD ; art. 3, 1) de la Directive police-justice.
[89] Art. 4, 1), du RGPD ; art. 3, 1) de la Directive police-justice.

apparence ou d'autres éléments spécifiques. Dans la mesure où l'identité de ces personnes peut être établie sur la base de ces informations, il s'agit de données à caractère personnel[90].

55 Parmi les données à caractère personnel, figurent les « données sensibles ». Il s'agit de catégories particulières de données à caractère personnel soumises à un régime de protection spécifique en raison de leur caractère particulièrement sensible[91]. Les données biométriques traitées aux fins d'identifier une personne physique de manière unique sont considérées comme des données sensibles[92]. Elles sont définies comme des données à caractère personnel « résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques »[93]. Nous reviendrons sur cette notion lorsque sera abordé le débat autour de la qualification des données traitées par le dispositif expérimental de VSA mis en place pour les JO 2024 en tant que données biométriques (voy. *infra* n[os] 78 et s.).

56 Quant à la notion de traitement, elle désigne « 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 »[94]. À cet égard, la définition légale cite entre autres la collecte des données à caractère personnel, leur enregistrement, leur utilisation, leur conservation ou encore leur consultation par les autorités compétentes. Toutes ces opérations seront vraisemblablement effectuées dans le cadre de l'expérimentation durant les JO 2024.

Section 2. Les garanties du droit dérivé de l'UE relatif à la protection des données à caractère personnel

57 Dans la mesure où la VSA peut constituer un traitement de données à caractère personnel, elle est soumise aux garanties prévues par le droit de la protection des données à caractère personnel. Nous examinerons ici les garanties faisant écho aux risques identifiés précédemment posés par la VSA (voy. *supra* n[os] 11 et s.), à savoir le principe de minimisation des données (§1), l'exactitude des données ainsi que sa tension avec la garantie du « privacy by design » (§2), la sécurité du traitement (§3), le contrôle humain (§4), les obligations de transparence et d'information reposant sur le responsable de traitement (§5) et les analyses d'impact (§6).

§1. Le principe de minimisation des données

58 Selon le principe de minimisation des données, les données à caractère personnel doivent être « adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées »[95]. Cela implique donc que seules les données essentielles à la réalisation du traitement soient traitées, et non toutes les données disponibles[96].

59 Dans le cas de la VSA, il est particulièrement complexe de respecter cette obligation. En effet, le système filme et analyse généralement la foule dans son ensemble. En raison des importantes difficultés que soulèvent la vidéosurveillance et à plus forte raison, la VSA à cet égard, leur utilisation ne peut être envisagée qu'après avoir rigoureusement déterminé que cette mesure est tout d'abord appropriée pour atteindre l'objectif souhaité, mais surtout qu'elle est

---

[90] E.D.P.B., « Guidelines 3/2019 on processing of personal data through video devices », disponible sur https://edpb.europa.eu , 10 juillet 2019, p. 5.
[91] Considérant 51 du RGPD.
[92] Art. 9, §1[er] du RGPD.
[93], art. 4, 14) du RGPD ; art. 3, 13) art. 3, 1) de la Directive police-justice.
[94] Art. 4, 2) du RGPD ; art. 3, 2) art. 3, 1) de la Directive police-justice.
[95] Art. 5, §1[er], c) du RGPD ; art. 4, §1[er], de la Directive police-justice.
[96] C. LEQUESNE ROTH, « New Surveillance Technologies… », *op. cit.*, p. 66.

nécessaire et proportionnée à ce dernier (voy. *infra* n^{os} 104 et s.)[97]. Le cas échéant, il faut alors jouer sur le nombre de caméras et leur caractère fixe ou mobile, étant entendu qu'une caméra mobile collecte plus de données. L'Autorité de protection des données espagnole recommande également de flouter certaines parties des images pour en limiter le traitement[98].

Un problème au niveau du principe de minimisation des données semble se profiler pour le dispositif expérimental envisagé pour les JO 2024, qui par nature collecte de nombreuses informations et de surcroît repose sur la captation d'images par des caméras mobiles équipées par des drones (voy. *supra* n° 35). 60

§2. L'exactitude des données et l'exigence du « privacy by design »

Le principe d'exactitude des données impose que les données traitées soient « exactes »[99], ce qui implique que les résultats produits par le système d'IA soient fiables lorsqu'ils portent sur des personnes concernées. 61

Comme souligné précédemment, la fiabilité de ces systèmes repose sur la qualité des jeux de données d'entraînement, apprenant à ces derniers ce que sont des comportements ou des évènements anormaux (voy. *supra* n° 23), et des données captées, sur la base desquelles se font les signalements (voy. *supra* n° 29). Or, obtenir des données de qualité se révèle parfois une tâche laborieuse, tant pour l'entraînement que pour le déploiement du système en situations réelles[100]. En France, il existe par ailleurs un risque accru à cet égard en raison du manque de jeux d'entraînement et de la faiblesse des réseaux de caméras équipées[101]. 62

En outre, une tension existe entre le principe d'exactitude et le principe du « privacy by design », lui aussi reconnu en droit de la protection des données[102]. Pour que la VSA respecte ce dernier, la CNIL recommande entre autres l'abaissement de la qualité des images, le floutage des images et une approche frugale des données[103]. Or, ces mesures diminuent la qualité des données, portant ainsi atteinte à la fiabilité du système. Ce faisant, elles risquent d'augmenter le nombre de faux positifs et de neutraliser la finalité même des systèmes. L'analyse coût-avantage du dispositif pour les forces de l'ordre risque ainsi d'en prendre un coup[104]. 63

§3. La sécurité du traitement et la violation des données

Le RGPD et la directive police-justice impose aux responsables de traitement de mettre en place des mesures pour garantir un niveau de sécurité adapté au risque que le traitement pose en termes de droits et libertés des personnes physiques[105]. Ce risque est extrêmement grave pour les catégories particulières de données, dont les données biométriques font partie[106]. En cas de violation des données, à comprendre comme une divulgation accidentelle ou malicieuse de ces 64

---

[97] E.D.P.B., « Guidelines 3/2019… », *op. cit.*, p. 8.
[98] A.E.P.D., « Guía sobre el uso de videocámaras para seguridad y otras finalidades », disponible sur https://www.aepd.es, 29 juin 2018, p. 8 et 9.
[99] Art. 5, §1er, d) du RGPD ; art. 4, §1er, d) de la Directive police-justice.
[100] C. GARVIE, « A Forensic Without the Science: Face Recognition in U.S. Criminal, Investigations », *Georgetown Law*, 2022, p. 18.
[101] 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.
[102] Art. 25, du RGPD.
[103] CNIL, « Caméras dites 'intelligentes'… », *op. cit.*, p. 13.
[104] C. LEQUESNE ROTH et J. KELLER, *op. cit.*, p. 67.
[105] Art. 32 du RGPD ; art. 29 de la Directive police-justice.
[106] C. LEQUESNE ROTH et J. KELLER, *op. cit.*, p. 65.

dernières[107], le responsable du traitement doit la notifier à l'autorité de contrôler, en précisant la nature des données concernées et les mesures préexistantes à la violation ainsi que celles prises pour pallier ses effets[108]. L'article 10 de la loi relative aux JO 2024 n'appelle pas à commentaire sur ce point, en ce qu'il se borne à énoncer que les données traitées « font l'objet de mesures de sécurisation appropriées »[109].

65 Comme souligné précédemment, en dépit des mesures mises en place, ces systèmes sont souvent vulnérables et peuvent être piratés (voy. *supra* n° 30). La violation de certaines données traitées par VSA, dont les données biométriques, est pourtant particulièrement grave. Rappelons à cet égard que les données biométriques ne peuvent pas être répudiées : une personne ne peut donc pas en changer (voy. *supra* n° 31). Le signalement de cette violation à l'autorité de contrôle n'est donc pas une solution satisfaisante. Or, en l'absence d'une solution palliant les difficultés évoquées, le traitement de certaines catégories de données devrait donc être strictement limité[110].

§4. L'absence de traitement automatisé

66 En principe, une personne physique a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé de ses données, sauf si un tel traitement est autorisé par le droit de l'Union ou des États membres et que des mesures appropriées pour sauvegarder les droits de la personne concernée sont prévues[111]. Cela implique donc qu'en l'absence d'une disposition contraire à ce qui précède, la VSA doit faire intervenir un humain dans la décision.

67 Cette garantie d'une intervention humaine se retrouve dans la loi relative aux JO 2024, aux côtés de l'exigence d'un contrôle humain permanent[112]. Pourtant, elle risque d'entrer en tension avec l'environnement managérial des services publics, dont la quête d'efficacité risque d'amoindrir la portée et d'accroitre la dépendance des agents vis-à-vis de ces systèmes (voy. *supra* 26 et s.). Le risque est en effet de déléguer aveuglément un problème – sensible – de sécurité à un système d'IA pour des motifs économiques[113]. De fait, assurer un contrôle humain concret implique des investissements significatifs, notamment dans la formation des agents. En matière de reconnaissance faciale, une étude a démontré que le contrôle humain était inadéquat en raison des biais des agents, renforcés par les biais du système d'IA. En outre, les agents auraient dû être formés pendant six mois à temps plein pour être capables d'identifier effectivement des visages qui ne leur étaient pas familiers[114]. Si le texte de la loi relative aux JO 2024 fait mention d'une formation des agents recevant les signalements[115], sa portée est à déterminée ultérieurement. Il semble néanmoins improbable qu'une formation aussi substantielle soit délivrée aux agents en raison de l'horizon proche des jeux.

§5. Les obligations de transparence et d'information

68 En vertu du RGPD le responsable du traitement est tenu à une obligation de transparence[116], dont l'obligation d'information est le corollaire, à l'égard de l'information préalable des

---

[107] C. LEQUESNE ROTH et J. KELLER, *ibidem*, p. 73
[108] Art. 33 RGPD ; art. 30 de la Directive police-justice.
[109] L. n°2023-380, 19 mai 2023, précitée, art. 10, VI, al. 1, 1°.
[110] C. LEQUESNE ROTH et J. KELLER, *op. cit.*, p. 74.
[111] Art. 22 du RGPD ; art. 11 de la Directive police-justice.
[112] L. n°2023-380, 19 mai 2023, précitée, art. 10, IV, al. 2 et 3.
[113] J. BLANES et R. HAILLARD, « "Nous risquons d'avaliser des usages technologiques controversés sans aval démocratique" (Caroline Lequesne-Roth) », *aefinfo*, 7 juillet 2023.
[114] C. GARVIE, *op. cit.*, p. 24.
[115] L. n°2023-380, 19 mai 2023, précitée, art. 10, V, al 2.
[116] Art. 5, §1 a) du RGPD ; Ce principe n'est pas consacré dans la directive police-justice.

personnes concernées. Le principe de transparence implique que les informations et les communications concernant le traitement de ces données soient aisément accessibles, compréhensibles et exprimées de manière claire et simple pour les personnes concernées[117]. Les articles 12 à 14 du RGPD établissent une obligation d'information et détaillent les informations à fournir au moment de collecter des données à caractère personnel – directement ou indirectement – auprès de la personne concernée. En ce sens, ces dispositions mettent en pratique le principe de transparence.

69 À cet égard, l'article 10 de la loi relative aux JO 2024 prévoit « une information générale du public sur l'emploi de traitements algorithmiques sur les images collectées » ainsi qu'une information du public « par tout moyen approprié de l'emploi de traitements algorithmique au moyen de systèmes de vidéoprotection ». Ces deux mesures de publicité semblent relever respectivement du principe de transparence et de l'obligation d'information prévue par l'article 14 du RGPD.

70 La manière dont cette publicité sera concrètement organisée pose néanmoins question. Face à la nécessaire accessibilité de l'information sur la VSA se confronte la complexité de cette technologie. Si le Groupe de travail de l'Article 29 recommande l'utilisation de visuels, de graphiques ou de logos pour assurer cette accessibilité à l'ensemble des publics, y compris aux « personnes vulnérables »[118], cette solution ne peut être répliquée pour la VSA. De fait, au-delà d'un problème d'exhaustivité de l'information[119], la VSA est une technologie complexe dont le fonctionnement et les enjeux sont difficilement réductibles à une simple infographie[120]. À cela, s'ajoute l'obstacle de la propriété intellectuelle et des secrets d'affaires, invoqués par les entreprises mandatées par les autorités pour développer ces systèmes, afin de refuser de communiquer les éléments techniques de ces derniers[121].

§6. Les analyses d'impact pour la protection des données

71 Le RGPD et la directive police-justice prévoient également une obligation reposant sur le responsable du traitement de réaliser une « Analyse d'Impact pour la Protection des Données » (ci-après « AIPD »), qui doit nécessairement précéder le déploiement de certains traitements de données personnelles[122]. Une AIPD répond à un double objectif : (i) définir et évaluer les risques pour les données personnelles du traitement pour atténuer les risques qui lui sont inhérents ; et, (ii) mettre en place un outil de gestion, d'évaluation et de prévention des risques en classant les garanties à fournir pour protéger les droits des personnes concernées par ordre de priorité[123]. Elle est obligatoire 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. »[124] Comme il a été souligné tout au long de cette étude, c'est le cas de la VSA qui présente un risque d'atteinte disproportionnée aux droits et libertés des citoyens, dont

---

[117] Cons. 39 du RGPD.
[118] G29, « Lignes directrices sur la transparence au sens du règlement (UE) 2016/679 », WP 260 rev. 01, disponible sur https://ec.europa.eu, 11 avril 2018.
[119] Toutes les informations figurant aux articles 12 à 14 du RGPD ne pourraient en toute vraisemblance ne pas y figurer ; C. LEQUESNE ROTH et J. KELLER, *op. cit.*, p. 63.
[120] Voy. not. L. CRANOR *et al.*, « A "Nutrition Label" for Privacy », *Symposium On Usable Privacy and Security*, 2009, p. 1 à 12.
[121] Voy. par exemple Trib., arrêt *Breyer c. Agence exécutive européenne pour la recherche*, 15 décembre 2022, T-158/19, EU:T:2021:902 ; C. LEQUESNE ROTH et J. KELLER, *op. cit.*, p. 63.
[122] Art. 35 du RGPD ; art. 27 de la Directive police-justice.
[123] C. LEQUESNE ROTH et J. KELLER, *op. cit.*, p. 69.
[124] Art. 35 du RGPD ; art. 27 de la Directive police-justice.

le droit à la vie privée et à la protection des données à caractère personnel, particulièrement lorsqu'elle est déployée dans les espaces publics à des fins sécuritaires.

72 La réalisation d'une AIPD est par ailleurs envisagée dans l'article 10 de la loi relative aux JO 2024. Celle-ci accompagnera le décret fixant les caractéristiques essentielles du traitement par VSA envisagé pour l'expérimentation[125] et sera ensuite actualisée lorsque le système de VSA développé sera autorisé[126].

73 S'il est heureux que la loi prévoie cette AIPD, cette dernière risque cependant de ne pas jouer son rôle essentiel à la mise en œuvre de garanties à cause de diverses lacunes inhérentes aux AIPD prévues par le droit de la protection des données à caractère personnel. La critique note à cet égard deux défauts majeurs : (i) des méthodologies variables menant à des niveaux de protection inégaux et (ii) une appréciation discrétionnaire du responsable de traitement, qui devient juge et partie dans l'évaluation des risques du traitement[127].

74 Sur le volet méthodologique, il convient de noter que le Comité Européen de la Protection des Données (ci-après « l'EDPB ») et le Contrôleur européen de la protection des données (ci-après « l'EDPS ») ne fournissent pas de méthodologie standardisée[128], menant à des approches divergentes selon l'autorité de protection des données formulant ses recommandations à ce sujet. Ainsi, certaines d'entre elles préconisent une analyse des risques se concentrant sur les droits et libertés, tandis que d'autres mettent l'accent sur les risques techniques et la cybersécurité[129]. Cette incertitude méthodologique mène ainsi à de l'insécurité juridique[130].

75 Quant à l'appréciation discrétionnaire du responsable de traitement, l'EDPS note que l'opportunité de réaliser une AIPD est appréciée par les responsables de traitement, ce qui constitue une faille dans le droit de la protection des données à caractère personnel. Ces derniers n'hésitent pas à minimiser ou ignorer sciemment certains risques pour se libérer d'une telle obligation. De même, dans l'AIPD, les risques tendent également à être minimisés et les mesures d'atténuation sont décidées en tenant compte des intérêts du responsable de traitement[131].

Section 3. La VSA et les données biométriques

76 Selon ses applications, la VSA peut traiter des données à caractère personnel, parmi lesquelles pourraient figurer des données biométriques. Or, comme évoqué ci-avant, en raison de leur nature particulièrement sensible, leur traitement est soumis à un régime juridique plus strict que celui applicable aux données à caractère personnel non sensibles. Ce faisant, il peut paraître opportun de recourir à des applications de la VSA ne traitant pas de telles données. C'est le choix qu'a opéré la France dans le cadre de la surveillance des JO 2024. En principe, selon l'article 10 de la loi relative aux JO 2024, le dispositif expérimental de VSA mis en place pour les jeux ne devrait pas traiter des données biométriques. Des voix se sont pourtant élevées

[125] L. n°2023-380, 19 mai 2023, précitée, art. 10, V, al. 3.
[126] L. n°2023-380, 19 mai 2023, précitée, art. 10, VII, al. 2.
[127] C. LEQUESNE ROTH et J. KELLER, *op. cit.*, p. 71 et 72.
[128] C. LEVALLOIS-BARTH et J. KELLER, « Analyse d'impact relative à la Protection des Données : le cas des voitures connectées », disponible sur https://cvpip.wp.imt.fr, 18 novembre 2021, p. 34 et 35.
[129] C. LEVALLOIS-BARTH, J. KELLER, op cit.. p. 80 et 81.
[130] C. LEQUESNE ROTH et J. KELLER, *op. cit.*, p. 71.
[131] E.D.P.S., « Survey on Data Protection Impact Assessments », disponible sur https://edps.europa.eu, 6 juillet 2020, p. 14.

au sein de la société civile clamant le contraire. Selon elles, cette interdiction serait contredite par l'objet même des traitements envisagés[132].

77 Les dissensions entre le gouvernement français, soutenu par la CNIL, et la société civile sur la qualification des données traitées par VSA en tant que données biométriques au sens du droit de l'UE de la protection des données sont l'occasion de revenir sur cette notion, relative à une technologie qui a fort évolué depuis. Au travers du cas d'étude de la loi relative aux JO 2024, seront examinées les conditions de cette qualification (§1). Dans la mesure, où la VSA peut traiter des données biométriques, il convient de rappeler brièvement le régime applicable à de tels traitements. Sous ce dernier, le traitement des données biométriques est en principe interdit (§2). Toutefois, la VSA pourrait bénéficier d'une exemption si elle respecte les exigences de nécessité et de proportionnalité (§3).

§1. La qualification des données traitées par VSA en tant que données biométriques

78 De la définition des données biométriques en droit européen de la protection des données (voy. *supra* n° 55), il ressort que des données, outre leur caractère personnel, doivent remplir trois conditions pour être considérées comme telles. Elles doivent résulter d'un traitement technique spécifique (A), se rapporter aux caractéristiques physiques, physiologiques ou comportementales d'une personne (B) et être traitées à des fins d'identification unique de la personne (C).

A. Des données à caractère personnel résultant d'un traitement technique spécifique

79 S'agissant du traitement technique spécifique, cette notion figure dans la définition légale des données biométriques, sans pour autant que sa portée y soit précisée. La seule indication fournie concerne la finalité de ce traitement, qui doit être l'identification unique d'une personne (voy. *infra* n^{os} 92 et s.).

80 La notion étant relativement vague, la doctrine l'a déconstruite en deux éléments. D'un part, dès lors qu'il est question d'un traitement, ce dernier doit être compris comme un traitement de données à caractère personnel au sens de l'article 4, paragraphe 2, du RGPD (voy. *supra* n° 56). D'autre part, son caractère technique et spécifique impliquerait que le traitement soit propre à la technologie de la biométrie[133]. Une telle interprétation implique de se plonger dans les traitements techniques que subissent les caractéristiques biométriques, à comprendre comme des attributs physiques ou comportementaux qui sont propres à une personne (voy. *infra* n° 84), pour être transformées en données utilisées par la suite pour identifier ou vérifier l'identité d'une personne.

81 Traditionnellement, ce processus se décompose en trois étapes[134]. Premièrement, au cours de l'étape d'enrôlement, les caractéristiques biométriques sont capturées et stockées sous la forme d'un échantillon biométrique, généralement sous la forme d'une image[135]. Deuxièmement, les informations de l'échantillon sont extraites, réduites et transformées en étiquettes ou en nombres à l'aide d'un algorithme. Au cours de cette phase, seules les informations discriminantes essentielles à la reconnaissance de la personne sont conservées. Ces informations sont ensuite stockées dans un gabarit biométrique, lequel est une

---

[132] HUMAN RIGHTS WATCH, *op. cit.*

[133] C. JASSERAND, « Legal Nature of Biometric Data: From 'Generic' Personal Data to Sensitive Data », *University of Groningen Faculty of Law Research Paper Series*, 2018, p. 9.

[134] C. JASSERAND, *op. cit.*, p. 9.

[135] ISO/IEC 2382-37, Terme 37.03.21, disponible sur https://www.iso.org/standard/55194.html, décembre 2012, cité par C. JASSERAND, *ibidem*, p. 10.

représentation mathématique de la caractéristique biométrique originale[136]. Troisièmement, au cours de la phase de comparaison, un nouvel échantillon biométrique est présenté à une caméra ou un capteur et est comparé à un gabarit précédemment enregistré de la même caractéristique biométrique. Dans certains cas, la comparaison peut être effectuée avec un autre échantillon biométrique au lieu d'un gabarit, bien que cela soit moins courant[137].

82 Ces différentes phases constituent plusieurs opérations de traitement au sens de l'article 4, paragraphe 2, du RGPD. Lors de la première, les données sont collectées. Ensuite, elles sont organisées, structurées, adaptées et stockées. Enfin, la dernière phase implique la récupération, la consultation, l'utilisation et la divulgation des données[138].

83 Ces étapes se retrouvent dans la VSA. Le volet de la vidéosurveillance permet en effet la collecte des données, alors que la composante algorithmique du dispositif traduit dans un premier temps les images en données pour ensuite les comparer à des modèles qui lui ont été présenté comme représentant des situations normales. Le traitement technique spécifique coïnciderait ainsi au recours à des outils analytiques[139] que la biométrie et la VSA présentent toutes deux. L'exigence de données résultant d'un traitement technique spécifique semble donc remplie. Ce n'est d'ailleurs pas l'aspect le plus contentieux du débat, qui s'est essentiellement concentré sur l'existence d'un traitement de données relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne (voy. *infra* n^{os} 84 et s.) et sur la notion d'identification unique (voy. *infra* n^{os} 92 et s.)

B. Des données à caractère personnel relatives à des caractéristiques physiques, physiologiques ou comportementales d'une personne

84 Outre ce qui précède, les données doivent se rapporter aux caractéristiques physiques, physiologiques ou comportementales d'une personne. Ce critère fait référence aux caractéristiques biométriques. La formulation employée par le texte permet de reconnaître qu'un large éventail de caractéristiques humaines mesurables peuvent être utilisées dans les technologies biométriques[140].

85 La définition légale de données biométriques reprend la traditionnelle distinction entre les caractéristiques physiques et physiologiques et celles comportementales. Les premières se rapportent à des caractéristiques relativement stables du corps humain[141]. Elles incluent notamment le visage, les empreintes digitales, l'ADN, la forme des oreilles, l'iris, la rétine, la géométrie de la main et la voix[142]. Les caractéristiques comportementales sont quant à elles associées au comportement ou aux mesures dynamiques d'un individu[143]. Elles sont considérées

---

[136] J. LARMOUTH, « Biometric Template », *Encyclopedia of Biometrics*, S. Z. Li et A. K. Jain (dir.), *s.l.*, Springer, 2015, p. 152 ; A. ADLER et S. SCHUCKERS, « Biometric Vulnerabilities, Overview », *Encyclopedia of Biometrics*, S. Z. Li et A. K. Jain (dir.), *s.l.*, Springer, 2015, p. 164.
[137] E. KINDT, *Privacy and Data Protection Issues of Biometric Applications, A Comparative Legal Analysis*, *s.l.*, Springer, 2013, p. 43 à 47.
[138] C. JASSERAND, *op. cit.*, p. 9 et 10.
[139] C. WENDEHORST et Y. DULLER, « Biometric Recognition and Behavioural Detection: Assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces », disponible sur https://www.europarl.europa.eu, 6 août 2021, p. 68.
[140] C. JASSERAND, *op. cit.*, p. 12.
[141] T. SABHANAYAGAM, V. PRASANNA VENKATESAN et K. SENTHAMARAIKANNAN, « A Comprehensive Survey on Various Biometric Systems », *International Journal of Applied Engineering Research*, 2018, p. 2276.
[142] G29, « Opinion 3/2012 on developments in biometric technologies », WP193, disponible sur https://ec.europa.eu, 27 avril 2012, p. 5.
[143] T. SABHANAYAGAM, V. PRASANNA VENKATESAN et K. SENTHAMARAIKANNAN, *op. cit.*, p. 2276.

comme des techniques de biométrie de seconde génération, aussi appelé « biométrie douce », en raison de leur capacité moindre à identifier un individu. Il s'agit typiquement de la signature manuscrite et de la démarche[144]. Peuvent également être considérés comme des caractéristiques comportementales l'activité cérébrale, ainsi que le clignement des yeux, l'augmentation de la rougeur du visage ou la direction des mouvements de la tête, lesquels sont des caractéristiques utilisées dans le cadre de la détection d'émotions[145].

Notons que le développement des caractéristiques biométriques comportementales rend de plus en plus difficile le traçage d'une ligne de démarcation claire entre ce qui constitue une caractéristique biométrique et ce qui constitue de simples caractéristiques discriminantes, permettant de différencier différentes classes ou catégories de personnes, qui sont utilisées dans le profilage de personnes physiques, par exemple[146]. Cela pourrait expliquer une certaine confusion lors des débats parlementaires sur la loi relative aux JO 2024, durant lesquels un parlementaire a, par exemple, allégué qu'identifier une personne par ses vêtements relevait de la biométrie[147]. 86

Il semble donc nécessaire de rappeler que de manière générale, les caractéristiques dites biométriques doivent présenter un certain degré d'immuabilité, c'est-à-dire que la personne physique concernée n'a que peu ou pas de chances de modifier les caractéristiques ou les signaux analysés[148]. Cette permanence est surtout prégnante dans les caractéristiques physiques et physiologiques, lesquelles sont particulièrement sensibles en raison de l'impossibilité pour un individu de les répudier. En effet, une fois la donnée compromise, elle l'est généralement définitivement et ne peut en principe pas être remplacée[149]. Toutefois, elle se retrouve également à un degré moindre dans les caractéristiques comportementales, sur lesquelles l'individu n'a qu'un degré de contrôle variable mais généralement faible. Ainsi, le fait qu'une personne porte un sweat à capuche rouge, ce qui permet de l'identifier sur un flux d'images, n'est pas une caractéristique biométrique, bien qu'il s'agisse d'une caractéristique discriminante. Cette personne peut bien plus aisément se défaire de son vêtement, qu'il peut, par exemple, altérer sa démarche ou ses maniérismes. Rien n'exclut cependant que le port d'un vêtement puisse être considéré comme une donnée sensible, puisqu'il pourrait révéler certaines informations sensibles sur la personne, mais il ne s'agira pas d'une donnée biométrique. 87

Si les vêtements que portent une personne ne constituent pas une caractéristique biométrique, cela ne signifie pas pour autant que la VSA ne traite pas de données relatives à des caractéristiques biométriques. Pour le déterminer, deux approches existent. La première est fonctionnelle. Suivant celle-ci, l'existence d'un tel traitement dépend des usages auxquels sont destinés la VSA. Cette approche est celle adoptée par la CNIL qui considère ainsi qu'une caméra augmentée filmant la voie publique pour classer les différents usages (voitures, vélos, etc.) ne remplit pas la condition de la nature « biométrique » des données traitées. Par contre, la détection de bagarres dans une foule implique bien l'analyse de caractéristiques physiques, physiologiques ou comportementales[150]. 88

---

[144] G29, « Opinion 3/2012… », *op. cit.* p.5.
[145] C. WENDEHORST et Y. DULLER, *op. cit.*, p. 14 et 21.
[146] C. WENDEHORST et Y. DULLER, *ibidem*, p. 21.
[147] Projet de loi relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions, Discussion des articles, *J.O.R.F.*, Assemblée nationale, 2022-2023, n°220, p. 2937.
[148] C. WENDEHORST et Y. DULLER, *op. cit.*, p. 21.
[149] D. RYJOUKHINA, *op. cit.*, p. 12.
[150] CNIL, « Caméras dites 'augmentées' dans les espaces publics : la position de la CNIL », disponible sur https://www.cnil.fr, 19 juillet 2022.

89 La seconde est une approche « par objet », à savoir qu'il suffirait qu'une personne soit filmée pour que ses caractéristiques biométriques soient traitées. Celle-ci est défendue par la société civile. Elle se fonde sur l'argument que le traitement algorithmique d'images contenant des personnes qu'opère la VSA aboutira nécessairement au traitement de caractéristiques biométriques, car le concepteur du programme n'a pas de maîtrise sur la sélection des variables et des caractéristiques qui déterminent le résultat fourni par la machine. En effet, la délimitation des caractéristiques que l'IA utilisera pour aboutir au résultat attendu n'est effectuée par un humain que dans des cas relativement simples, ce qui n'est pas le cas de la VSA. En raison de sa complexité, elle fonctionne grâce à des algorithmes de *deep learning*. Pour créer le modèle, à partir duquel la machine fournira des résultats, ces derniers analysent les images contenant des personnes filmées et *a fortiori* leurs données comportementales, physiques et physiologiques. Ces informations de nature biométrique font donc partie de l'ensemble des données dont les algorithmes peuvent inférer le modèle. Or, dans le cadre du *deep learning*, les caractéristiques et les variables retenues pour réaliser le modèle sont en principe déterminées par les algorithmes-mêmes. Aucun humain n'intervient pour les empêcher de sélectionner telle variable qui se fonde sur une caractéristique biométrique[151]. Cela serait par ailleurs presque impossible pour le concepteur en raison de l'effet « boîte noire » des modèles créés par *deep learning*, dont la complexité est telle qu'il pratiquement impossible de les comprendre[152].

90 L'application de l'approche par objet aboutit à un plus grand nombre de cas dans lesquels la VSA sera considérée comme traitant des données relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne. Pour qu'un tel traitement existe, il suffit en effet qu'une personne soit filmée et que les images sur lesquelles elle figure soient traitées. L'approche fonctionnelle de la CNIL est plus stricte. Elle requiert que la VSA soit utilisée aux fins d'analyser des personnes, dont leurs comportements, même si elles forment un groupe. Cette dernière nous semble néanmoins perdre de sa pertinence face au grand potentiel d'adaptabilité des technologies de VSA, qui permet de faire évoluer le dispositif vers d'autres usages – visant ou non l'analyse de personnes – parfois par simple clic (voy. *supra* n^{os} 17 et s.). `À cela s'ajoute sa redondance avec la condition de poursuite d'un but d'identification unique discutée ci-dessous (voy. *infra* n^{os} 92 et s.).

91 Si le décret français[153] établissant une liste d'événements prédéterminés qu'il est envisagé de traiter par VSA n'a pas encore été adopté, le gouvernement français indique cependant que pourraient figurer parmi ceux-ci « la présence d'objets abandonnés sur la voie publique, le port apparent ou l'utilisation d'armes, le non-respect d'un sens de circulation, le franchissement d'un périmètre d'interdiction ou la présence d'une personne ou d'un véhicule dans un périmètre d'interdiction ou une zone sensible, la présence d'une ou plusieurs personnes au sol, certains mouvements de foule et phénomènes de concentration de personnes ainsi que les départs de feu ou émanations de fumées »[154]. Selon l'approche par objet, la presque totalité des situations décrites entraînent le risque qu'une personne soit filmée et que les images sur lesquelles elle figure soient traitées. Même à suivre l'approche de la CNIL, certains de ces évènements conduiraient à une utilisation de la VSA à des fins d'analyse des personnes[155]. Par conséquent,

---

[151] LA QUADRATURE DU NET, Contribution extérieure dans l'affaire n°2023-850 DC, devant le Conseil constitutionnel, du 17 mai 2023.

[152] Voy. not. à ce sujet : J. BURELL, « How the machine 'thinks': Understanding opacity in machine learning algorithms », *Big Data & Society*, 2016, p. 1 à 12.

[153] Un décret est un acte réglementaire de droit français ; Const. (française), 4 octobre 1958, art. 21 et 37.

[154] Observations du Gouvernement dans l'affaire n°2023-850 DC, devant le Conseil constitutionnel, du 17 mai 2023, p. 13 ; voy. également Étude d'impact précitée, Sén., 2022-2023, n°220, p. 112.

[155] Nous visons ici particulièrement les situations suivantes : l'utilisation d'armes, le non-respect d'un sens de circulation, le franchissement d'un périmètre d'interdiction ou la présence d'une ou plusieurs personnes au sol,

le critère d'un traitement de données relatives à des caractéristiques physiques, physiologiques ou comportementales d'une personne semble rempli.

C. Des données à caractère personnel dont le traitement permet ou confirme l'identification unique d'une personne

92 Enfin, le traitement doit confirmer ou permettre l'identification unique de la personne. Ce critère décrit les finalités de l'utilisation des caractéristiques biométriques, à partir desquelles les données biométriques sont extraites[156]. Pour la CNIL, il s'agit là du critère principal distinguant les caméras biométriques des simples caméras augmentées de la VSA[157].

93 Les termes « confirmer ou permettre » l'identification unique d'une personne font écho à une distinction que le considérant 51 du RGPD opère entre l'authentification et l'identification au sens strict. L'authentification[158] est une comparaison « un à un » (1 :1), qui consiste à comparer le gabarit « réel » d'une personne qui prétend avoir une identité particulière avec le gabarit lié à cette identité, qui est stocké dans une base de données. L'objectif est de confirmer que la personne est bien celle qu'elle prétend être. Le dispositif européen de contrôle du passage aux frontières PARAFE où les gabarits stockés dans les passeports biométriques des voyageurs sont comparés à ceux que réalisent des portiques dédiés[159] en est un exemple. Par opposition à l'authentification, l'identification au sens strict opère une comparaison « d'un à plusieurs » (1 : n), où l'identité d'une personne est établie en faisant correspondre son gabarit « réel » avec des gabarits stockés dans une base de données. En d'autres termes, l'identification vise à établir qui est la personne et non à vérifier qu'elle est celle qu'elle prétend être[160]. Un système biométrique d'identification au sens strict a par exemple été utilisé en Italie pour lutter contre l'immigration illégale[161].

94 Dans le cas de la VSA telle qu'elle est envisagée dans le cadre de l'expérimentation pour les JO 2024, le débat s'est cristallisé autour de l'identification qu'opèrerait ou non le dispositif. Le gouvernement français défendait qu'il ne pouvait être question d'identification dès lors que la VSA visait à chaque fois à signaler des événements, et non des individus[162]. La société civile avançait, quant à elle, que pour remplir son objectif, la VSA devait nécessairement isoler des personnes par rapport à leur environnement, ce qui constituerait une « identification unique » [163]. À l'appui, elle invoquait un avis du Comité Européen de la Protection des Données (ci-après « l'EDPB ») sur la vidéosurveillance, qui déclare que « si un responsable du traitement souhaite détecter une personne concernée qui pénètre à nouveau dans l'espace surveillé ou dans une autre zone (par exemple, pour projeter une publicité personnalisée continue), la finalité serait alors d'identifier de manière unique une personne physique, ce qui signifie que

---

et enfin certains mouvements de foule et phénomènes de concentration de personnes.

[156] C. JASSERAND, *op. cit.*, p. 12.

[157] CNIL, « Caméras dites 'augmentées'… », *op. cit.*

[158] Le terme « vérification » correspond davantage à la terminologie utilisée par les experts en biométrie. Par pédagogie, nous continuerons néanmoins d'utiliser le terme légal d'« authentification » ; C. JASSERAND, *op. cit.*, p. 12.

[159] MINISTÈRE DE L'INTÉRIEUR, « PARAFE : passer les contrôles aux frontières plus rapidement », disponible sur https://www.interieur.gouv.fr, 4 avril 2019.

[160] C. WENDEHORST et Y. DULLER, *op. cit.*, p. 19 et 20.

[161] Il s'agit du système de reconnaissance faciale SARI, en Italie, qui opérait en temps réel des comparaisons sur la base d'une « liste de surveillance » contenant jusqu'à 10 000 images de visages ; G.D.P.P., « Riconoscimento facciale: Sari Real Time non è conforme alla », disponible sur https://www.garanteprivacy.it, 16 avril 2021.

[162] Observations du Gouvernement dans l'affaire n°2023-850 DC, devant le Conseil constitutionnel, du 17 mai 2023, p. 13.

[163] HUMAN RIGHTS WATCH, *op. cit.*

l'opération relèverait d'emblée de l'article [9]. »[164] De ce dernier, il ressort qu'associer à une personne une empreinte numérique pour la reconnaître – et éventuellement la suivre – sans nécessairement que son identité civile y soit liée, relève de l'identification unique[165].

95 Sans disposer du cahier des charges formalisant les exigences du dispositif qui sera mis en place, il est difficile d'affirmer que ce dernier procédera ou non à une identification unique. Des usages que le gouvernement a explicitement reconnus (voy. *supra* n°91), une majorité apparait comme ne nécessitant pas d'isoler des personnes particulières. Pour ces derniers, il suffit de déterminer qu'il s'agit d'un être humain. Toutefois, pour d'autres, en particulier le port apparent ou l'utilisation d'armes, il semble difficile de concevoir que le gouvernement accepterait un simple signalement d'attention, sans une fonctionnalité permettant de suivre la personne signalée comme portant une arme ou l'utilisant. Rappelons que l'objectif de la VSA est d'améliorer l'efficacité des interventions de services concernés. Il semble donc improbable que le gouvernement écarte des fonctionnalités permettant aux agents d'effectuer une action ciblée sur la personne dont le comportement ou le corps est analysé pour déclencher un « évènement révélant un risque pour la sécurité des personnes ».

96 En outre, la définition des données biométriques en droit de la protection des données est devenue désuète au fil des progrès technologiques en matière de biométrie. Aux systèmes d'authentification et d'identification visés par le RGPD, s'ajoutent deux autres types de technologies biométriques : la catégorisation et la détection[166]. Ces dernières sont apparues récemment avec l'essor de la biométrie de seconde génération et sont visées dans le projet de l'*AI Act*. Ce dernier définit un système de catégorisation biométrique comme « un système d'IA destiné à affecter des personnes physiques à des catégories spécifiques selon le sexe, l'âge, la couleur des cheveux, la couleur des yeux, les tatouages, l'origine ethnique ou l'orientation sexuelle ou politique, etc., sur la base de leurs données biométriques »[167]. Le terme « détection biométrique » fait références aux techniques biométriques dont l'objectif est de détecter des émotions ou des intentions de personnes physiques sur la base de leurs données biométriques[168]. Elle est plus communément appelée « reconnaissance des émotions ».

97 Dans un rapport sur les technologies biométriques, le Défenseur des droits donne comme exemple de système de catégorisation la détection de comportements suspects pour lutter contre les vols dans les supermarchés, par exemple[169]. En l'espèce, il est apparent que l'expérimentation envisagée touchera au moins partiellement à de la catégorisation biométrique, puisqu'il s'agira de traiter des données relatives à des caractéristiques physiques, physiologiques ou comportementales d'une personne pour la catégoriser comme adoptant un comportement suspect.

98 Que penser alors du paragraphe IV de l'article 10 de la loi qui déclare que « [l]es traitements mentionnés au I du présent article n'utilisent aucun système d'identification biométrique, ne traitent aucune donnée biométrique et ne mettent en œuvre aucune technique de reconnaissance faciale » ? En se référant strictement à la notion de données biométriques en droit de la protection des données, cette affirmation n'est pas nécessairement incorrecte. Toutefois, cela implique que dans les faits, les fonctionnalités du dispositif ne permettent en aucun cas

---

[164] E.D.P.B., « Lignes directrices sur les vidéos contenant des données personnelles 3/201 », disponible sur https://edpb.europa.eu, 29 janvier 2020, p. 19.
[165] LA QUADRATURE DU NET, *Projet de loi…, op. cit.*, p. 36 à 37.
[166] C. WENDEHORST et Y. DULLER, *op. cit.*, p. 21.
[167] Art. 3, 35) de l'*AI Act*.
[168] Art. 3, 34) de l'*AI Act*.
[169] DÉFENSEUR DES DROITS, « Technologies biométriques : l'impératif respect des droits fondamentaux », disponible sur https://www.defenseurdesdroits.fr, 19 juillet 2021, p. 6.

d'attribuer une empreinte numérique à une personne spécifique pour la reconnaitre et la suivre au travers de l'espace surveillé, ce qui est improbable. Par contre, il est en contradiction avec l'état de l'art des systèmes biométriques, que la définition du RGPD et de la directive police-justice n'a pas réussi à suivre, et risque également d'entrer en conflit avec le futur règlement sur l'intelligence artificielle de l'UE.

§2. Le régime des données biométriques du RGPD et de la directive police-justice

99 Comme évoqué ci-avant, en raison de la nature particulièrement sensible des données biométriques, celles-ci sont soumises à un régime juridique distinct des données à caractère personnel non sensibles. Il existe en effet une interdiction de principe de traiter les données biométriques[170]. Cette dernière connaît néanmoins des exceptions, permettant de fonder le déploiement d'un traitement biométrique, qui varient selon l'instrument applicable[171].

100 Dans le RGPD, pléthore d'exceptions existent. Nous retenons cependant celle prévue à l'article 9, paragraphe 2, g) que le RGPD partage avec la directive police-justice[172] et qui est sans doute celle qui sera invoquée par des Etats souhaitant déployer des systèmes d'identification biométrique. Cette dernière autorise le traitement de données biométriques lorsque des motifs d'intérêt public important le nécessitent, sur base du droit de l'Union ou du droit national. Les dispositions autorisant le traitement devront en outre être proportionnées à l'objectif poursuivi et respecter l'essence du droit à la protection des données. Enfin, des mesures visant à garantir les droits fondamentaux et les intérêts de la personne concernée doivent également être prévues à cet égard[173]. Ces conditions doivent être interprétée à la lumière de la Charte et en particulier des conditions de l'article 52, paragraphe 1er,[174] évoquées ci-avant (voy. *supra* nos 42 et s.).

101 Cette exemption légale se retrouve également dans la directive police-justice, bien qu'en des termes légèrement différents. Une attention particulière y est portée à l'exigence de nécessité, qui doit être absolue[175]. En outre, des garanties appropriées pour les droits et libertés de la personne concernée doivent être prévues. Le caractère approprié de celles-ci s'examine à la lumière de leur capacité à protéger les personnes contre le risque de discrimination[176]. Enfin, le traitement doit nécessairement être autorisé par le droit de l'Union ou le droit national « pour protéger les intérêts vitaux de la personne concernée ou d'une autre personne physique » ou « lorsque le traitement porte sur des données manifestement rendues publiques par la personne concernée »[177]. Selon le Groupe de travail sur l'article 29, ces deux situations doivent néanmoins être interprétées comme illustrant simplement des cas dans lesquels le droit pourrait prévoir un tel traitement et non comme étant limitatives[178].

---

[170] Art. 9, §1er du RGPD.
[171] Pour un exposé plus détaillé sur l'applicabilité de ces exceptions, voy. C. LEQUESNE ROTH et J. KELLER, *op. cit.*, p. 49 à 55.
[172] C. LEQUESNE ROTH et J. KELLER, *ibidem*, p. 51.
[173] Art. 9, §2, g) du RGPD.
[174] E.D.P.B., « Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement », disponible sur https://edpb.europa.eu, 12 mai 2022, p. 20.
[175] G29, « Opinion on some key issues of the Law Enforcement Directive (EU 2016/680) », WP 258, disponible sur sur https://ec.europa.eu, 7 décembre 2017, p. 8.
[176] C. FORGET, « La protection des données dans le secteur de la "police" et de la "justice" », *Le règlement general sur la protection des données (RGPD/GDPR)*, C. de Terwangne et K. Rosier (dir.), Bruxelles, Larcier, 2018, p. 888 et 889 ; G29, « Opinion on some key issues… », *op. cit.*, p. 8.
[177] Art. 10 de la Directive police-justice.
[178] G29, « Opinion on some key issues… », *op. cit.*, p. 7.

102 Ce fondement a néanmoins été critiqué pour la trop grande marge d'appréciation laissée aux Etats-membres en la matière. La législation européenne ne fournit en effet aucune indication sur la manière dont l'intérêt public « important » ou la nécessité « absolue » doivent être appréciés. Or, cette liberté nationale d'interprétation engendre un double problème : d'une part, la protection des données biométriques risque de varier considérablement selon les Etats-membres ; d'autre part, l'intérêt public étant une notion élastique, certaines juridictions pourraient l'invoquer pour poursuivre des projets risqués[179]. À ce titre, le précédent créé par la France à l'échelle de l'UE en votant une loi organisant un arsenal de surveillance à grande échelle dans l'espace public qui sera très probablement biométrique – et ce en dépit de la lettre de celle-ci – est dangereux.

103 Pour que le déploiement d'un dispositif de VSA soit conforme au droit dérivé de l'UE relatif à la protection des données à caractère personnel, les traitements de données à caractère personnel – parfois biométriques – doivent avoir un fondement. Comme établi précédemment, lorsque la VSA risque de traiter des données biométriques, ce dernier sera manifestement celui de l'exemption légale consacrée à l'article 9, paragraphe 2, g) du RGPD et à l'article 10, a), de la directive police-justice. Celle-ci soustrait un traitement de données biométriques à l'interdiction de principe de traiter ces dernières, moyennant le respect de certaines conditions examinées ci-après au travers du cas français.

§3. L'exemption légale pour le traitement de données biométriques : la nécessité et la proportionnalité du traitement

104 L'exemption d'un traitement de données biométriques de l'interdiction de principe de les traiter est possible moyennant le respect de conditions analogues à celles de l'article 52, paragraphe 1er de la Charte. À la différence de cette dernière, le RGPD et la directive police-justice insistent particulièrement sur la nécessité dont doit pouvoir attester un traitement de données biométriques au travers des formulations « lorsque des motifs d'intérêt public important le nécessitent »[180] et « uniquement en cas de nécessité absolue »[181], ainsi que sur les garanties qui doivent l'entourer. Mis à part le respect de la légalité déjà examinée précédemment (voy. *supra* nos 44 et 45), le bénéfice de l'exemption semble donc reposer sur une analyse plus stricte du caractère nécessaire et proportionnée du traitement.

105 Le principe de nécessité impose de procéder à une évaluation factuelle de l'efficacité de la mesure par rapport à l'objectif poursuivi et de déterminer si cette mesure est moins intrusive par rapport aux autres moyens de réaliser ce dernier[182]. Si la mesure proposée prévoit le traitement de données sensibles, telles que les données biométriques, l'évaluation de l'efficacité se doit d'être plus rigoureuse. L'attention particulière accordée à la nécessité dans la formulation des articles 9, paragraphe 2, g) du RGPD et 10, a), de la directive police-justice indique que la marge d'appréciation laissée aux autorités chargées de l'application de la loi dans le cadre de l'examen de la nécessité est limitée au strict minimum[183].

106 Dans le cas de l'expérimentation française de la VSA dans le cadre des JO 2024, certains ont invoqué un défaut de nécessité par rapport à l'objectif poursuivi, à savoir de détecter, en temps réel, des événements prédéterminés susceptibles de présenter ou de révéler des « risques

---

[179] C. LEQUESNE ROTH et J. KELLER, *op. cit.*, p. 52.
[180] Art. 9, §2, g) du RGPD.
[181] Art. 10 de la Directive police-justice.
[182] E.D.P.S., « Lignes directrices du CEPD portant sur l'évaluation du caractère proportionné des mesures limitant les droits fondamentaux à la vie privée et à la protection des données à caractère personnel », disponible sur https://edps.europa.eu, 20 décembre 2019, p. 5.
[183] E.D.P.B., « Guidelines 05/2022… », *op. cit.*, p. 19.

d'actes de terrorisme ou d'atteintes graves à la sécurité des personnes » pour assurer la sécurité des manifestations sportives, récréatives et culturelles. Selon eux, ni les travaux préparatoires à la loi, ni les débats parlementaires ne démontrent l'efficacité de la mesure. De fait, aucun élément de preuve scientifiquement vérifiable n'a été produit pour illustrer comment ils pourraient éventuellement atteindre l'objectif poursuivi, de façon certaine et efficace[184]. Au contraire, un récent rapport d'information qualifie de « contrastés » les résultats des dernières expérimentations autour des caméras intelligentes réalisées en France[185].

Par ailleurs, il n'a pas non plus été démontré en quoi les moyens actuels ne suffiraient pas à remplir cet objectif[186]. À cet égard, rappelons que les pouvoirs de surveillance des autorités françaises se sont considérablement étendus depuis les attentats de 2015. Ainsi, en 2017, la France a adopté une loi[187] faisant entrer dans le droit commun pénal et administratif certaines mesures de surveillance appliquées dans le cadre de l'état d'urgence, exceptionnellement déclaré à la suite des attentats, et en expérimentant d'autres – elles-mêmes pérennisées ultérieurement[188] – aux fins de renforcer la sécurité intérieure et la lutte contre le terrorisme. Au surplus, notons également des affaires pendantes contre la France devant la Cour européenne des droits de l'homme dénonçant des mesures de surveillance de masse[189]. Avec plus de 90.000 caméras sous le contrôle de la police et de la gendarmerie disséminées à travers le territoire[190], l'appareil de surveillance français est donc loin d'être dérisoire. 107

S'agissant du principe de proportionnalité, ce dernier exige l'existence de garanties suffisantes permettant « de réduire à un niveau "acceptable"/proportionné les risques posés par la mesure envisagée au regard des droits fondamentaux et des libertés des individus concernés »[191]. 108

De récentes affaires portant sur des technologies analogues à la VSA, telle qu'elle est autorisée par la loi française relative aux JO 2024, démontrent l'importance de cette exigence à l'ère des Big Data. Au Royaume-Uni, 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 l'article 8 de la Convention européenne des droits de l'homme. La Cour a jugé le cadre juridique « insuffisant », au sens où les raisons pour lesquelles une personne pouvait être placée sur la liste de surveillance, à partir de laquelle le dispositif fonctionne, n'étaient pas claires. De même, il n'existait pas de critères pour déterminer où ce dernier pouvait être 109

---

[184] LA QUADRATURE DU NET, Contribution extérieure dans l'affaire n°2023-850 DC, devant le Conseil constitutionnel, du 17 mai 2023, p. 6 et 7.

[185] P. GOSSELIN et P. LATOMBE, Assemblée nationale, Session 2022-2023, Rapport d'information n°1089, fait au nom de la commission des lois constitutionnelles, de législation et de l'administration générale de la République, sur les enjeux de l'utilisation d'images de sécurité dans le domaine public dans une finalité de lutte contre l'insécurité, enregistré le 12 avril 2023, p. 64.

[186] LA QUADRATURE DU NET, Contribution extérieure dans l'affaire n°2023-850 DC, devant le Conseil constitutionnel, du 17 mai 2023, p. 6 et 7.

[187] L. n° 2017-1510, 30 octobre 2017, renforçant la sécurité intérieure et la lutte contre le terrorisme (« SILT »), NOR : INTX1716370L.

[188] La loi permet le traitement algorithmique des données de connexion pour détecter les menaces, introduit une réforme de l'accès aux archives publiques et élargit les critères de fermeture administrative des lieux de culte, soupçonnés d'être liés à des faits de nature terroriste ; L. n° 2021-998, 30 juillet 2021, relative à la prévention d'actes de terrorisme et au renseignement, NOR : INTD2107675L.

[189] Voy. à cet égard les affaires pendantes : Association confraternelle de la presse judiciaire c. France et 11 autres requêtes (n° 49526/19/15) Follorou c. France (n° 30635/17) et Johannes c. France (n° 30636/17).

[190] P. GOSSELIN et P. LATOMBE, *op. cit.*, p. 25 et 26.

[191] E.D.P.S., « Lignes directrices du CEPD portant sur l'évaluation du caractère proportionné… », *op. cit.*, p. 11 et 12.

déployé[192]. En Allemagne, la Cour constitutionnelle a épinglé les législations des *Länder* de Hesse et d'Hambourg concernant un dispositif d'analyse automatisée de données personnelles afin de prévenir des troubles à l'ordre public, créé par l'entreprise américaine Palantir. Elle insiste sur la sévérité de l'atteinte aux droits fondamentaux que le traitement algorithmique des données collectées pourrait engendrer et sur l'importance de l'élaboration du cadre juridique à cet égard. En l'espèce, elle met en cause le manque de limites dans ce dernier au sujet du type et de la quantité de données qui peuvent être traitées par le dispositif, ainsi que sur les méthodes utilisées pour analyser et interpréter celles-ci[193].

110 À l'inverse des législations en cause dans ces affaires, la loi relative aux JO 2024 offre de nombreuses garanties dans son article 10, validées par la CNIL[194]. Le Conseil constitutionnel, amené à se prononcer sur un recours contre cette dernière, a par ailleurs invoqué l'encadrement strict que prévoit l'article 10 pour conclure au respect de l'exigence de proportionnalité[195]. Parmi les garanties citées par le Conseil constitutionnel, figure la limitation du dispositif de VSA à certaines manifestations qui par leurs ampleurs de fréquentation ou par leurs circonstances sont particulièrement exposées à des risques d'actes de terrorisme ou d'atteintes graves à la sécurité des personne[196]. Il évoque également le paragraphe IV interdisant le traitement de données biométriques et le rapprochement avec d'autres fichiers[197], ainsi que l'absence de décision automatique[198], reprise des articles 22 du RGPD et 11 de la directive police-justice[199].

111 L'approche du Conseil constitutionnel est cependant très formaliste. Elle ne prend pas en compte le contexte dans lequel cette expérimentation s'inscrit. Comme établi précédemment, la garantie d'une absence de traitement de données biométriques tient formellement la route, mais il est en réalité peu probable que le gouvernement s'y tienne au vu des finalités en jeu (voy. *supra* n° 98). Du reste, la garantie d'un contrôle humain sera en tension avec l'environnement managérial des services publics et le problème de la dépendance humaine aux outils d'IA (voy. *supra* n° 27). En ce sens, elle ne semble pas en l'état former une garantie appropriée au risque que les systèmes de VSA posent.

112 À l'issue de cet exposé, il semble difficile d'argumenter que les exigences de nécessité et de proportionnalité sont effectivement respectées. En outre, comme établi ci-dessus, la VSA ne permet par nature pas d'offrir des garanties solides sur d'autres aspects du droit de la protection des données à caractère personnel.

Titre III. VERS UN MEILLEUR ENCADREMENT DE LA VSA PAR L'*AI ACT* ?

113 Si le droit de la protection des données semble dépassé par les derniers développements en matière d'IA, le projet de l'*AI Act*, présenté par la Commission le 21 avril 2021, se profile comme la solution pour mieux encadrer les systèmes d'IA. Ce dernier se trouve actuellement à la dernière étape du processus législatif européen, à savoir les trilogues entre le Conseil de l'UE, le Parlement et la Commission.

---

[192] [2020] EWCA Civ 1058, n° C1/2019/2670, §90 et 91.
[193] BVerfG, Urteil des Ersten Senats, BvR 1547/19 et BvR 2634/20, 16 février 2023.
[194] CNIL, « Jeux olympiques et paralympiques 2024 : la CNIL publie son avis sur le projet de loi », disponible sur https://www.cnil.fr, 4 janvier 2023.
[195] Conseil constitutionnel, 17 mai 2023, n°2023-850 DC, points n°36 à 46.
[196] Conseil constitutionnel, 17 mai 2023, n°2023-850 DC, point 37.
[197] Conseil constitutionnel, 17 mai 2023, n°2023-850 DC, point 42.
[198] Conseil constitutionnel, 17 mai 2023, n°2023-850 DC, point 43.
[199] Étude d'impact précitée, Sén., 2022-2023, n°220, p. 113.

L'*AI Act* repose sur une approche fondée sur les risques que présente un système d'IA. Le projet distingue (i) les IA présentant un risque inacceptable, lesquelles sont interdites, (ii) celles à haut risque, soumises à une série d'obligations, (iii) celles à risque limité, seulement soumises à des obligations de transparence et enfin, (iv) celles ne présentant qu'un risque minimal, exemptes de toute obligation. À notre sens, la VSA pourrait tomber dans la première (Chapitre 1) et la deuxième catégorie (Chapitre 2). 114

Chapitre 1. La VSA comme système d'IA présentant un risque inacceptable

La VSA, lorsqu'elle est utilisée à des fins répressives dans des espaces publics par les autorités et selon les usages concrets auxquels elle est destinée, risque d'être considérée soit comme une IA présentant un risque inacceptable, soit comme une IA à haut risque. Dans la première hypothèse, bien que l'*AI Act* dans sa version originale[200] interdise 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 », le recours à la VSA ne sera pas forcément prohibé en raison des nombreuses exceptions prévues. Ainsi un dispositif de VSA qui, comme le permettra probablement celui de l'expérimentation française, rend possible le suivi d'une personne portant une arme dans l'espace surveillé pourrait être autorisé car son utilisation relève de « 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 »[201]. De même, 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[202]. Cette possibilité sera sans doute largement utilisée par les États comme le laisse un projeter une récente proposition de loi en France, autorisant sans détour le recours à la reconnaissance faciale dans les espaces publics[203]. 115

Le Parlement européen a substantiellement amendé cette partie du projet en interdisant simplement l'utilisation de systèmes d'identification biométrique à distance « en temps réel », sans prévoir d'exceptions[204]. Cette initiative est heureuse eu égard aux risques que ces technologies posent en matière de droits fondamentaux, particulièrement lorsqu'elles sont utilisées par les autorités. Le projet original de l'*AI Act* contient des exceptions trop larges, que l'EDPB et l'EDPS dénoncent dans un avis conjoint. Selon eux, la menace sécuritaire sera presque toujours « suffisamment élevée » pour justifier l'utilisation continue de ces derniers[205]. Or, en application des principes de nécessité et de proportionnalité, le recours à de telles technologies devrait être strictement limité – temporellement et géographiquement – et réservé à des circonstances exceptionnelles. 116

Chapitre 2. La VSA comme système d'IA à haut risque

Pour le reste, la VSA peut également être considérée comme une IA à haut risque. À considérer que catégoriser une personne comme adoptant un comportement anormal – comme le fait la VSA – relève du profilage[206], elle tomberait alors sous la définition « les systèmes 117

---

[200] Celle proposée par la Commission le 21 avril 2021.
[201] Art. 5, (d), (ii) de l'*AI Act*.
[202] Art. 5, §4 de l'*AI Act*.
[203] Proposition de loi relative à la reconnaissance biométrique dans l'espace public, Sén., 2022-2023, n°505.
[204] PARLEMENT EUROPÉEN, Communiqué de presse, « AI Act: a step closer to the first rules on Artificial Intelligence », 11 mai 2023.
[205] E.D.P.B. et E.D.P.S., « Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) », disponible sur https://edpb.europa.eu ,18 juin 2021.
[206] La définition du profilage inclut en effet l'analyse du comportement par des traitements automatisés ; voy. art. 4, 4) du RGPD.

d'IA destinés à être utilisés par les autorités répressives pour le profilage de personnes physiques visé à l'article 3, paragraphe 4, de la directive (UE) 2016/680 dans le cadre d'activités de détection, d'enquête ou de poursuite relatives à des infractions pénales »[207] ou plus généralement « les systèmes d'IA destinés à être utilisés pour l'identification biométrique à distance «en temps réel» et «a posteriori» des personnes physiques »[208] font partie.

118 L'*AI Act* impose certaines garanties à l'utilisation des systèmes d'IA, en particulier ceux à haut risque, qui pourraient être intéressantes face aux lacunes du droit de la protection des données évoquées ci-avant. Ainsi, seront examinées l'exigence d'un « système de gestion des risques » inscrivant l'analyse d'impact dans le cycle de vie du système d'IA (Section 1), la garantie d'un contrôle humain (Section 2), les obligations de transparence s'imposant aux IA à haut risque et à risque limité (Section 3) et ainsi que celle en matière d'exactitude, de robustesse et de cybersécurité (Section 4).

Section 1. Le système de gestion des risques et l'analyse d'impact des droits fondamentaux

119 L'article 9 de l'*AI Act* prévoit un « système de gestion des risques », impliquant à l'instar d'une analyse d'impact, l'identification et l'analyse des risques associés au système d'IA à haut risque, ainsi que l'adoption de mesures pour les atténuer. Cette obligation repose sur le fournisseur du système d'IA[209]. Si le fournisseur n'est pas nécessairement le responsable de traitement, un problème analogue à celui constaté dans les AIPD se pose (voy. *supra* n° 75). Le fournisseur a en effet intérêt à minimiser les risques du système d'IA qu'il fournit pour le commercialiser. En outre, l'*AI Act* opte pour une neutralité méthodologique et n'impose ainsi aucun standard à cet égard. Ce faisant, dans sa version originale, il souffre des mêmes défauts que les AIPD, dont l'incertitude méthodologique cause une insécurité juridique (voy. *supra* n° 74).

120 Le Parlement européen a cependant amendé le texte sur ce point, en ajoutant une obligation pour l'utilisateur du système d'IA de réaliser une analyse d'impact des droits fondamentaux, complémentaire à l'AIPD. Si cette obligation ne résout pas la probable partialité de l'analyse, elle a le bénéfice de réintroduire la question des droits fondamentaux, qui était parfois sciemment écartée par les responsables de traitement dans des AIPD se focalisant principalement sur les aspects techniques. Il est donc à espérer que cette nouvelle obligation survive aux trilogues, comme cela semble être attendu[210], sans être vidée de sa substance.

Section 2. Le contrôle humain

121 L'*AI Act* introduit une garantie d'un contrôle humain plus poussée que celle existant en droit de la protection des données à caractère personnel. Le texte exige un contrôle humain effectif, pendant la période d'utilisation d'un système d'IA à haut risque. L'objectif est de contrôler que son usage est conforme à sa destination, et, en cas de mauvaise utilisation, de le reconfigurer, voire de l'arrêter. Concrètement, ce contrôle est assuré par une personne avec niveau de compétence suffisant pour « appréhender totalement les capacités et les limites du système d'IA », « avoir conscience d'une éventuelle tendance à se fier automatiquement ou excessivement aux résultats produits », « interpréter correctement les résultats du système

[207] Annexe III, point 6, f) de l'*AI Act*.
[208] Annexe III, point 1, a) de l'*AI Act*.
[209] Cons. 42 de l'*AI Act*.
[210] L. BERTUZZI, « EU policymakers prepare to close first aspects of AI regulation », *Euractiv*, 11 juillet 2023.

d'IA » et « décider, dans une situation particulière, de ne pas utiliser le système d'IA à haut risque »[211].

Ce contrôle humain « renforcé » répond à la critique adressée à la garantie de l'absence de traitement automatisé en droit de la protection des données : pour assurer un contrôle effectif, un individu doit bénéficier d'une solide formation (voy. *supra* n°67). Il est cependant important de noter que le contrôle humain pourrait se révéler inefficace, malgré une formation substantielle des personnes chargées de ce dernier. Le cas échéant, le recours à certains systèmes d'IA, dont pourrait faire partie la VSA, devrait être abandonné en raison d'un manque de garanties effectives pour mitiger les risques encourus par les personnes concernées[212]. 122

Section 3. La transparence et les obligations d'information

L'*AI Act* introduit des obligations de transparence pour les systèmes d'IA à haut risque et à risque limité[213]. En particulier, il introduit une obligation à charge des fournisseurs d'informer les personnes physiques qu'elles interagissent avec un système d'IA. Toutefois, cette dernière est rapidement tempérée par de larges exceptions concernant entre autres les systèmes d'IA pour la prévention/détection d'infraction pénale ou pour la reconnaissance des émotions ou d'un système de catégorisation biométrique[214]. La VSA se voit donc exclue de ce champ dans ses usages les plus intrusifs. 123

Une telle prise de position est inquiétante dès lors que le texte reconnait explicitement que pour les systèmes d'IA destinés à être utilisés dans un contexte répressif, « l'exactitude, la fiabilité et la transparence sont particulièrement importantes pour éviter les conséquences négatives, conserver la confiance du public et garantir que des comptes soient rendus et que des recours efficaces puissent être exercés »[215]. En ce sens, l'*AI Act* en l'état ne mitige pas les risques soulevés ci-avant au sujet de l'opacité des systèmes d'IA (voy. *supra* n^{os} 26 et s.). Pourtant, il nous semble important qu'un citoyen ait conscience que derrière les caméras qu'il voit dans la rue, se cache en réalité un système d'IA capable de l'analyser. Une personne ne sachant pas quand elle est effectivement surveillée, avec une intensité supérieure dans le cas de la VSA, risque de ressentir un sentiment de surveillance constante, l'amenant à s'autocensurer ou à ne pas exercer un droit qui lui est légitimement accordé, par crainte d'une sanction ou d'une atteinte à son intimité[216]. Le risque d'atteinte aux droits fondamentaux est donc élevé. 124

Section 4. Exactitude, robustesse et cybersécurité

L'*AI Act* prévoit des exigences plus techniques en matière de sécurité que le RGPD et la directive police-justice. Outre une obligation de transparence sur « *le niveau d'exactitude, de robustesse et de cybersécurité* » du système d'IA[217], le texte exige une sécurité informatique renforcée, dès la conception et par défaut, en fonction de sa destination, qui doit être maintenue pendant toute la durée d'utilisation de l'IA. De même, l'*AI Act* insiste sur la menace des attaques de tiers et impose une certaine proportionnalité entre les risques posés par le système d'IA et les mesures de sécurité mises en place. Enfin, lorsqu'un système d'IA poursuit son apprentissage, une fois déployée, des mesures visant à prévenir l'empoisonnement de données 125

---

[211] S'agissant des « systèmes d'identification biométrique à distance », aucune mesure ou décision ne peut être prise par l'utilisateur « sur la base de l'identification résultant du système sans vérification et confirmation par au moins deux personnes physiques » ; art. 14 de l'*AI Act*.
[212] C. LEQUESNE ROTH et J. KELLER, *op. cit.*, p. 68.
[213] Art. 13, 14 et 52 de l'*AI Act*.
[214] Art. 52, §1 et 2 de l'*AI Act*.
[215] Cons. 38 de l'*AI Act*.
[216] Voy. en ce sens, C. LEQUESNE ROTH et J. KELLER, *op. cit.*, p. 45.
[217] Art. 13 § 3 (ii) de l'*AI Act*.

doivent être mises en place afin d'éviter, entre autres, de porter atteinte à la fiabilité du système et le cas échéant, de produire des résultats discriminatoires[218].

126 Ces garanties semblent de nature à offrir un niveau de sécurité[219] et de fiabilité supérieur à celui mis en place par le droit de la protection des données à caractère personnel.

CONCLUSION

127 Entre le risque de surveillance de masse, les possibles dérives, le potentiel quasi-illimité d'usages des technologies de VSA et les risques inhérents au recours à l'IA sur laquelle elles se fondent, leur encadrement strict est une condition *sine qua non* à leur déploiement à des fins sécuritaires par les autorités publiques dans les espaces accessibles au public, sous peine de graves atteintes aux droits fondamentaux. À cet égard, la législation actuelle en matière de protection des données à caractère personnel semblait la plus à même à fournir des garanties satisfaisantes. Toutefois, cette dernière se confronte à la collecte nécessairement massive des données des personnes concernées pour assurer la fiabilité de ces technologies, à leur vulnérabilité face aux attaques tierces, ainsi qu'à leur opacité, d'origine technique et juridique.

128 Au-delà de cette incompatibilité par nature de la VSA avec certaines garanties issues du droit de la protection des données à caractère personnel, la biométrie n'est plus ce qu'elle était au moment de l'adoption du RGPD et de la directive police-justice. Ces instruments peinent donc à appliquer un régime plus strict à certaines applications de la VSA, pour lesquelles l'existence d'un traitement de données biométriques tel qu'ils le définissent est débattable. La loi française relative aux JO 2024 autorisant certaines applications de la VSA en est une illustration.

129 Face à de telles lacunes, le futur *AI Act* profile un meilleur encadrement, notamment en termes d'exactitude, de robustesse et de cybersécurité des systèmes de VSA. Toutefois, dans sa version originale, il ne limite pas suffisamment les cas dans lesquels ces technologies fort intrusives pourraient être utilisées et risque ainsi d'en autoriser l'utilisation constante. L'*AI Act* en l'état légitime en outre un manque de transparence pour certains systèmes de VSA, en ne créant aucune obligation d'informer les personnes qu'elles font l'objet d'un traitement par une IA. Le risque est ici de perdre la confiance du public et de susciter chez les citoyens un sentiment de surveillance constante.

130 Pour l'instant, cependant, les jeux ne sont pas encore faits. Le dispositif précis mis en place pour les JO 2024 n'a pas encore été arrêté et l'*AI Act* est en cours de négociation entre la Commission, le Parlement et le Conseil de l'UE. Il est encore temps d'arrêter *Big Brother*.

[218] Art. 15 de l'*AI Act*.
[219] C. LEQUESNE ROTH et J. KELLER, *op. cit.*, p. 66.

TABLE DES MATIERES

Introduction **1**

Titre I. Les contours de la VSA : cadre théorique et cas d'étude des JO 2024 ..... **2**

Chapitre 1. Cadre théorique 2

Section 1. La notion et les applications de la VSA 2

Section 2. Les avantages 3

Section 3. Les risques 3

Chapitre 2. Un cas d'étude : l'expérimentation de la VSA pour les JO 2024 9

Titre II. L'encadrement (lacunaire) de la VSA par le droit de la protection des données 10

Chapitre 1. Le droit primaire de l'UE : la Charte des droits fondamentaux de l'UE ... 10

Section 1. L'applicabilité de l'article 8 de la Charte 10

Section 2. La VSA comme limitation à l'article 8 de la Charte 11

Chapitre 2. Le droit dérivé de l'UE : le RGPD et la directive police-justice 13

Section 1. L'applicabilité du RGPD et de la directive police-justice 14

Section 2. Les garanties du droit dérivé de l'UE relatif à la protection des données à caractère personnel 15

Section 3. La VSA et les données biométriques 19

Titre III. Vers un meilleur encadrement de la VSA par l'*AI Act* ? 29

Chapitre 1. La VSA comme système d'IA présentant un risque inacceptable 30

Chapitre 2. La VSA comme système d'IA à haut risque 30

Section 1. Le système de gestion des risques et l'analyse d'impact des droits fondamentaux 31

Section 2. Le contrôle humain 31

Section 3. La transparence et les obligations d'information 32

Section 4. Exactitude, robustesse et cybersécurité 32

Conclusion **33**

Table des matières **34**

BIBLIOGRAPHIE

Législation

Union européenne

- Charte des droits fondamentaux de l'Union européenne, *J.O.C.E.*, C364, 18 décembre 2000.
- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), *J.O.U.E.*, L 119, 4 mai 2016.
- Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, *J.O.U.E.*, L119, 4 mai 2016.
- 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, 21 avril 2021.

France

- Const., 4 octobre 1958.
- L. n° 2017-1510, 30 octobre 2017, renforçant la sécurité intérieure et la lutte contre le terrorisme (« SILT »), NOR : INTX1716370L.
- L. n° 2021-998, 30 juillet 2021, relative à la prévention d'actes de terrorisme et au renseignement, NOR : INTD2107675L.
- L. n°2023-22, 24 janvier 2023, d'orientation et de programmation du ministère de l'intérieur (« LOPMI »), NOR : IOMD2223411L
- L. n°2023-380, 19 mai 2023, relative aux jeux Olympiques et Paralympiques de 2024, NOR : SPOX2233026L.
- Projet de loi relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions, Sén., 2022-2023, n°220.
- Proposition de loi relative à la reconnaissance biométrique dans l'espace public, Sén., 2022-2023, n°505.
- Projet de loi d'orientation et de programmation du ministère de l'intérieur, Sén., 2022-2023, n°876, NOR : INTD2204555L/Bleue-1

Jurisprudence

Cour de justice de l'Union européenne

- C.J. (gde ch.), arrêt *Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources et Kärntner Landesregierung*, 8 avril 2014, aff. jointes C-293/12 et C-594/12, EU:C:2014:238.
- C.J., arrêt *Schrems v. Data Protection Commissioner*, 8 octobre 2015, C-362/14, EU:C:2015:650.

– C.J., arrêt *WebMindLicenses c. Nemzeti Adó- és Vámhivatal Kiemelt Adó- és Vám Főigazgatóság*, 17 décembre 2015, C-419/14, EU:C:2015:832.

Cour européenne des droits de l'homme

– Cour. eur. D.H., arrêt *Malone c. Royaume-Uni*, 2 août 1984.
– Cour eur. D.H., arrêt *Rotaru c. Roumanie*, 4 mai 2000.
– Cour eur. D.H., arrêt *Gillan et Quinton c. Royaume-Uni*, 12 janvier 2010.
– Cour eur. D.H., arrêt *Shimovolos c. Russia*, 21 juin 2011.
– Association confraternelle de la presse judiciaire c. France et 11 autres requêtes (n° 49526/19/15).
– Follorou c. France (n° 30635/17).
– Johannes c. France (n° 30636/17).

Jurisprudence étrangère

– [2020] EWCA Civ 1058, n° C1/2019/2670
– BVerfG, Urteil des Ersten Senats, BvR 1547/19 et BvR 2634/20, 16 février 2023.
– Conseil constitutionnel, 17 mai 2023, n°2023-850.
– Observations du Gouvernement dans l'affaire n°2023-850 DC, devant le Conseil constitutionnel, du 17 mai 2023.
– AMNESTY, Contribution extérieure dans l'affaire n°2023-850, devant le Conseil constitutionnel, du 17 mai 2023.
– LA QUADRATURE DU NET, Contribution extérieure dans l'affaire n°2023-850, devant le Conseil constitutionnel, du 17 mai 2023.

Doctrine

– ADLER A. et SCHUCKERS S., « Biometric Vulnerabilities, Overview », *Encyclopedia of Biometrics*, S. Z. Li et A. K. Jain (dir.), *s.l.*, Springer, 2015, p. 160 à 168.
– ANASTASIOU T., KARAGIORGOU S., PETROU P., PAPAMARTZIVANOS D., GIANNETSOS T., TSIRIGOTAKI G. et KEIZER J., « Towards Robustifying Image Classifiers against the Perils of Adversarial Attacks on Artificial Intelligence Systems », *Sensors*, 2022, p. 6905 à 6927.
– BAROCAS S. et SELBST A., « Big Data's Disparate Impact », *California Law Review*, 2016, p. 671 à 732.
– BOSE J. et AARABI P., « Adversarial Attacks on Face Detectors using Neural Net based Constrained Optimization », *arXiv*, 2018, p. 1 à 6.
– BROWNE S., *Dark Matters: On the Surveillance of Blackness*, Durham, Duke University Press, 2015, p. 1 à 224.
– BUOLAMWINI J. et GEBRU T., « Proceedings of the 1st Conference on Fairness, Accountability and Transparency », *P.M.L.R.*, 2018, p. 77 à 91.
– J. BURELL, « How the machine 'thinks': Understanding opacity in machine learning algorithms », Big Data & Society, 2016, p. 1 à 12.
– CHARPENET J. et LEQUESNE ROTH C., « Discrimination et biais genrés, Les lacunes juridiques de l'audit algorithmique », *Recueil Dalloz*, 2019, p. 1852 à 1857.
– CHORAŚ M., PAWLICKI M., PUCHALSKI D. et KOZIK R., « Machine Learning – The Results Are Not the only Thing that Matters! What About Security, Explainability and Fairness? », *Computational Science – ICCS*, Krzhizhanovskaya V., Závodszky G., Lees M.

H., Dongarra J. J., Sloot P. M. A., Brissos S. et Teixeira J. (dir.), Cham, Springer, 2020, p. 615 à 628.
- CRANOR L., KELLEY P. G., BRESEE J. et REEDER R. W., « A “Nutrition Label” for Privacy », *Symposium On Usable Privacy and Security*, 2009, p. 1 à 12.
- DAUBRESSE M.-P., de BELENT A. et DURAIN J., 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, p. 1 à 136.
- DÉFENSEUR DES DROITS, « Technologies biométriques : l’impératif respect des droits fondamentaux », disponible sur https://www.defenseurdesdroits.fr, 19 juillet 2021, p. 3 à 19.
- DÉFENSEUR DES DROITS, « Perception du développement des technologies biométriques en France : entre manque d’information et demande d’encadrement », disponible sur https://www.defenseurdesdroits.fr, 6 octobre 2022, p. 2 à 15.
- DESCHESNE F., DIGNUM V., ZARDIASHVILI L. et BIEGER J., « AI & Ethics at the Police: Towards Responsible use of Artificial Intelligence in the Dutch Police », disponible sur https://scholarlypublications.universiteitleiden.nl, mars 2019, p. 3.
- FORGET, C., « La protection des données dans le secteur de la “police” et de la “justice” », *Le règlement général sur la protection des données (RGPD/GDPR)*, de Terwangne C. et Rosier K.(dir.), Bruxelles, Larcier, 2018, p. 865 à 900.
- GARVIE C., « A Forensic Without the Science: Face Recognition in U.S. Criminal, Investigations », *Georgetown Law*, 2022, p. 1 à 77.
- GILL M. et SPRIGGS A., « *Assessing the impact of CCTV* », disponible sur https://techfak.uni-bielefeld.de, février 2005, p. 1 à 176.
- GOSSELIN P. et LATOMBE P., Assemblée nationale, Session 2022-2023, Rapport d’information n°1089, fait au nom de la commission des lois constitutionnelles, de législation et de l’administration générale de la République, sur les enjeux de l’utilisation d’images de sécurité dans le domaine public dans une finalité de lutte contre l’insécurité, enregistré le 12 avril 2023, p. 1 à 152.
- JASSERAND C., « Legal Nature of Biometric Data: From ‘Generic’ Personal Data to Sensitive Data », *University of Groningen Faculty of Law Research Paper Series*, 2018, p. 1 à 24.
- KEYES O., « Automating autism: Disability, discourse, and Artificial Intelligence », *Journal of Sociotechnical Critique*, 2020, p. 1 à 31.
- KINDT E., *Privacy and Data Protection Issues of Biometric Applications, A Comparative Legal Analysis, s.l.*, Springer, 2013, p. 1 à 907.
- KOMKOV S. et PETIUSHKO A., « AdvHat: Real-world adversarial attack on ArcFace Face ID system », *arXiv*, 2019, p. 1 à 9.
- LA QUADRATURE DU NET, Projet de loi relatif aux Jeux Olympiques et Paralympiques de 2024 : dossier d’analyse de la vidéosurveillance automatisée, 21 janvier 2023, p. 1 à 49.
- LARMOUTH J., « Biometric Template », *Encyclopedia of Biometrics*, S. Z. Li et A. K. Jain (dir.), *s.l.*, Springer, 2015, p. 152.
- LENAERTS K., « Limits on Limitations: The Essence of Fundamental Rights in the EU », *German Law Journal*, 2019, p. 779 à 793.
- LEQUESNE ROTH C., « New Surveillance Technologies in Public Spaces Challenges and Perspectives for European Law at the Example of Facial Recognition », disponible

sur https://www.academia.edu, avril 2021, p. 1 à 96.
- LEQUESNE ROTH C. et KELLER J., « Livre blanc pour l'Observatoire de l'éthique publique : surveiller les foules, pour un encadrement des IA 'physiognomoniques' », disponible sur https://www.observatoireethiquepublique.com, 1er avril 2023, p. 1 à 86.
- LEVALLOIS-BARTH C. et KELLER J., « Analyse d'impact relative à la Protection des Données : le cas des voitures connectées », disponible sur https://cvpip.wp.imt.fr, 18 novembre 2021, p. 1 à 157.
- MANN M. et MATZNER T., « Challenging algorithmic profiling: The limits of data protection and anti-discrimination in responding to emergent discrimination », *Big Data & Society*, 2019, p. 1 à 11.
- RYJOUKHINA D., « Les données biométriques et l'identité — Quelle protection juridique pour ces données à caractère personnel ? », *R.D.T.I.*, 2018, p. 5 à 31.
- SABHANAYAGAM T., PRASANNA VENKATESAN V. et SENTHAMARAIKANNAN K., « A Comprehensive Survey on Various Biometric Systems », *International Journal of Applied Engineering Research*, 2018, p. 2276 à 2297.
- WENDEHORST C. et DULLER Y., « Biometric Recognition and Behavioural Detection: Assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces », disponible sur https://www.europarl.europa.eu, 6 août 2021, p. 1 à 104.
- ZABLOCKI M., GOŚCIEWSKA K., FREJLICHOWSKI D. et HOFMAN R., « Intelligent video surveillance systems for public spaces – a survey », *Journal of Theoretical and Applied Computer Science*, 2014, p. 13 à 27.

Sources institutionnelles

Agence des droits fondamentaux de l'Union européenne (A.D.F.)

A.D.F., *Manuel de droit européen en matière de protection des données*, Luxembourg, Office des publications de l'Union européenne, 2018, p. 1 à 450.

Autorités nationales de protection des données, à l'exception de la CNIL

- A.E.P.D., « Guía sobre el uso de videocámaras para seguridad y otras finalidades », disponible sur https://www.aepd.es, 29 juin 2018.
- G.D.P.P., « Riconoscimento facciale: Sari Real Time non è conforme alla », disponible sur https://www.garanteprivacy.it, 16 avril 2021.
- A.P.D., Recommandation relative au traitement de données biométriques, disponible sur www.autoriteprotectiondonnees.be, 1er décembre 2021.

Comité Européen de la Protection des Données (E.D.P.B.)

- E.D.P.B., « Guidelines 3/2019 on processing of personal data through video devices », disponible sur https://edpb.europa.eu , 10 juillet 2019.
- E.D.P.B., « Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement », disponible sur https://edpb.europa.eu, 12 mai 2022.
- E.D.P.B., « Lignes directrices sur les vidéos contenant des données personnelles 3/201 », disponible sur https://edpb.europa.eu, 29 janvier 2020.
- E.D.P.B. et E.D.P.S., « Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) », disponible sur https://edpb.europa.eu ,18

juin 2021.

Commission Nationale de l'Informatique et des Libertés (CNIL)

– CNIL, « Directive 'Police-Justice' : de quoi parle-t-on ? », disponible sur https://www.cnil.fr, 20 février 2019.
– CNIL, « Reconnaissance faciale : pour un débat à la hauteur des enjeux », disponible sur https://www.cnil.fr, 14 novembre 2019.
– CNIL, « Vidéoprotection : quelles sont les dispositions applicables ? », disponible sur https://www.cnil.fr, 13 décembre 2019.
– CNIL, « Caméras dites 'augmentées' dans les espaces publics : la position de la CNIL », disponible sur https://www.cnil.fr, 19 juillet 2022.
– CNIL, Délibération n° 2022-118 portant avis sur un projet de loi portant sur les jeux Olympiques et Paralympiques de 2024, 8 décembre 2022.
– CNIL, « Jeux olympiques et paralympiques 2024 : la CNIL publie son avis sur le projet de loi », disponible sur https://www.cnil.fr, 4 janvier 2023.

Contrôleur européen de la protection des données (E.D.P.S.)

– E.D.P.S., « Survey on Data Protection Impact Assessments », disponible sur https://edps.europa.eu, 6 juillet 2020.
– E.D.P.S., « Lignes directrices du CEPD portant sur l'évaluation du caractère proportionné des mesures limitant les droits fondamentaux à la vie privée et à la protection des données à caractère personnel », disponible sur https://edps.europa.eu, 20 décembre 2019.

Groupe de travail « Article 29 » sur la protection des données (G29)

– G29, « Lignes directrices sur la transparence au sens du règlement (UE) 2016/679 », WP 260 rev. 01, disponible sur https://ec.europa.eu, 11 avril 2018.
– G29, « Opinion on some key issues of the Law Enforcement Directive (EU 2016/680) », WP 258, disponible sur sur https://ec.europa.eu, 7 décembre 2017.

Autres

– COUR DES COMPTES, « Référé : Le plan de vidéoprotection de la préfecture de police de Paris », disponible sur https://www.ccomptes.fr, 10 février 2022, p. 1 à 7.
– INSTITUT PARIS RÉGION, « La sécurité à l'heure de l'intelligence artificielle », disponible sur https://www.institutparisregion.fr, 6 février 2020, p. 1 à 4.
– ISO/IEC 2382-37, Terme 37.03.21, disponible sur https://www.iso.org/standard/55194.html, décembre 2012.
– GROUPE D'EXPERTS INDÉPENDANTS DE HAUT NIVEAU SUR L'INTELLIGENCE ARTIFICIELLE, *Lignes directrices en matière d'éthique pour une IA digne de confiance*, 2019.
– MINISTÈRE DE L'INTÉRIEUR, « PARAFE : passer les contrôles aux frontières plus rapidement », disponible sur https://www.interieur.gouv.fr, 4 avril 2019.
– MINISTÈRE DE L'INTÉRIEUR, « Livre blanc de la sécurité intérieure », disponible sur https://www.interieur.gouv.fr, 16 novembre 2020,
– X, « Partie III — Champ d'application, interprétation et effets de la charte », disponible sur https://e-justice.europa.eu, 25 novembre 2020.

Divers

- BERTUZZI L., « EU Policymakers prepare to close first aspects of AI regulation », *Euractiv*, 11 juillet 2023.
- BLANES J. et HAILLARD R., « "Nous risquons d'avaliser des usages technologiques controversés sans aval démocratique" (Caroline Lequesne-Roth) », *aefinfo*, 7 juillet 2023.
- BURKE G., FEDERMAN J., WU H., KRUTIKA P. et McGUIRK R., « Police seize on COVID-19 tech to expand global surveillance », disponible sur https://apnews.com, 21 décembre 2022.
- CHAZAL C., « La vidéosurveillance est-elle efficace ? », *Le Monde*, 17 mai 2018.
- HUMAN RIGHTS WATCH, « Lettre de la société civile aux députés français sur le projet de loi relatif aux Jeux olympiques et paralympiques 2024 », disponible sur https://www.hrw.org/fr, 7 mars 2023.
- IBM, « Qu'est-ce que la Computer Vision ? », disponible sur https://www.ibm.com, *s.d.*, consulté le 7 juin 2023.
- LECLERC J.-M., « JO 2024 : Gérald Darmanin veut un dispositif sécuritaire digne d'un événement planétaire », *Le Figaro*, 26 octobre 2022.
- LO LUCA A., « Adversarial Machine Learning: Attacks and Possible Defense Strategies », disponible sur https://towardsdatascience.com, 1er août 2021.
- McGUIRK M., « Police in Australia co-opted COVID-19 apps to fight crime », disponible sur https://apnews.com, 20 décembre 2022.
- X, « Hauts-de-Seine les caméras espionnes de Levallois : Le système de vidéo-surveillance installé par le maire suscite des protestations », *Le Monde*, 14 mars 1993.
- X, « Théorie de l'apprentissage statistique », disponible sur https://fr.wikipedia.org, s.d., consulté le 7 juin 2023.