MASTER COMPLÉMENTAIRE EN DROIT DES TECHNOLOGIES NOUVELLES

Le déploiement de la vidéosurveillance algorithmique dans l'espace public en Europe
Sacrifice de libertés pour le fantasme d'une police prédictive ?

DOUTSIS, Zaphiro

Award date:
2023

Awarding institution:
Universite de Namur

Université de Namur

Faculté de droit

Le déploiement de la vidéosurveillance algorithmique dans l'espace public en Europe :

Sacrifice de libertés pour le fantasme d'une police prédictive?

Mémoire réalisé par :

Zaphiro DOUTSIS

Sous la supervision de :

Promotrice : Cécile DE TERWANGNE

Co-promoteur : Antoine DELFORGE

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. »

Remerciements

Je tiens à remercier toutes les personnes qui m'ont aidée dans la rédaction de ce mémoire.

Je remercie dans un premier temps ma promotrice de mémoire, Cécile de Terwangne, pour ses enseignements précieux, qui m'ont permis de développer mon esprit d'analyse et ma réflexion sur la protection de la vie privée.

Je souhaite également exprimer ma gratitude envers Antoine Delforge, qui m'a apporté son regard d'expert en la matière et qui m'a aidée à trouver le fil conducteur du présent travail.

Enfin, je remercie mes parents, Valérie et Nicolas, ainsi que ma grand-mère, Monique Schön, pour leur soutien inconditionnel. Je remercie également ma sœur, Sarah, et mes amis, qui ont toujours été là pour moi et dont les encouragements m'ont accompagnée dans la rédaction de ce mémoire.

A tous, je vous présente ma plus sincère gratitude.

Table des matières

Introduction

« Souriez, vous êtes filmés ! ». Partout où nous allons, nos yeux se posent sur cette fameuse phrase, accompagnée d'un pictogramme représentant une caméra de vidéosurveillance.

Si cette réalité nous frappait jusqu'alors le plus souvent dans les lieux privés, tels que des magasins, des salles de concerts ou encore dans une salle d'attente, cette technologie de surveillance tend à se démocratiser également dans nos rues.

Mais alors que nous sommes habitués à la vidéosurveillance dite traditionnelle, une autre forme de dispositif a vu le jour au sein de notre espace public : la vidéosurveillance algorithmique.

Ainsi, le présent travail aura pour objet de s'intéresser au déploiement de cette technologie au sein de la sphère publique. Nous nous concentrerons sur son utilisation par les forces de l'ordre en Europe dans le cadre d'un objectif de sécurité des citoyens.

De fait, le sujet est fort intéressant d'un point de vue juridique, en ce que cette numérisation de la vidéosurveillance nous amène à nous poser de nombreuses questions : *Qu'est-ce que la vidéosurveillance algorithmique et que recouvre-t-elle exactement ? Qui déploie les algorithmes utilisés par l'intelligence artificielle ? Quel encadrement juridique pour ce type de technologie ? Quelles conséquences pour nos libertés et notre société actuelle ? Quelles sont les dérives possibles ?*

Nous tenterons de répondre à ces questions, en scindant notre travail en deux parties.

En premier lieu, nous nous pencherons sur le cadre juridique actuel en Europe. Nous commencerons par nous intéresser à la notion de vidéosurveillance algorithmique, pour ensuite évoquer la protection des données à caractère personnel prévue par le RGPD mais également la proposition de loi européenne sur l'intelligence artificielle faite par la Commission , l'AI Act.

Nous clôturerons ce premier titre par des exemples d'utilisations de la vidéosurveillance algorithmique en Europe, en nous focalisant sur la France, et son projet pour les Jeux Olympiques et Paralympiques 2024, et sur la Belgique.

En second lieu, nous examinerons les limites du cadre posé par l'Union européenne. Plus concrètement, nous nous interrogerons sur les dérives possibles, avec une attention particulière accordée aux risques pour nos libertés fondamentales, aux risques de discrimination ou encore de surveillance de masse généralisée.

Enfin, nous illustrerons nos propos à la lumière de pays utilisant déjà ces technologies à grande échelle, tels que la Chine, l'Iran ou encore Israël. Des pistes de solutions seront également envisagées, afin de ne pas sombrer dans les dérives précitées.

Pour finir, une conclusion originale sera proposée au lecteur.

TITRE I. La vidéosurveillance algorithmique à l'heure actuelle en Europe

SECTION 1. ASPECTS TECHNIQUES DE LA VIDÉOSURVEILLANCE ALGORITHMIQUE

Avant toute chose, il nous faut comprendre de quoi nous allons parler. Ainsi, penchons-nous sur la notion de vidéosurveillance algorithmique (ci-après « VSA »): qu'est-ce et comment fonctionne-t-elle ?

§1. Notions: caméras « augmentées » vs. caméras « biométriques »

C'est alors que nous nous apercevons que la définition même du concept mène déjà à la controverse. En effet, selon la Commission nationale de l'informatique et des libertés (ci-après « CNIL »), il convient de distinguer caméras « biométriques » et caméras « augmentées »[1], alors que pour d'autres – comme la Quadrature du Net, par exemple – la VSA est en soit un outil de surveillance biométrique[2]. Commençons dès lors par faire le point sur ces deux notions.

Toujours selon la CNIL, « deux critères permettent de distinguer ces dispositifs :

- la nature des données traitées : caractéristique physique, physiologique ou comportementale ;

- l'objectif du dispositif : identifier ou authentifier de manière unique une personne »[3].

De fait, si la surveillance biométrique cumule les deux critères (*ex : reconnaissance faciale*), la caméra « augmentée », quant à elle, « n'en remplira aucun (*ex : une caméra « augmentée » qui filme la rue pour classer les différents usagers : voitures, vélos,…)* ou seulement un des deux (*ex : une caméra « augmentée » qui détecte les bagarres dans une foule*) »[4].

Ainsi, la principale différence est que la caméra « augmentée » a pour objectif de « catégoriser et d'analyser grâce à l'intelligence artificielle sans identifier une personne de manière unique »[5], à l'inverse de la caméra biométrique.

Il est important de comprendre les contours de cette distinction pour ses implications juridiques, notamment dans le cas où des données « sensibles » sont traitées. Nous y reviendrons ultérieurement.

§2. Tentative de définition de la vidéosurveillance algorithmique

Mais alors, *à quelle catégorie appartient la VSA ?* Selon la CNIL, la « vidéo augmentée désigne ici des dispositifs vidéo auxquels sont associés des traitements algorithmiques mis en œuvre

[1] CNIL, « Caméras dites « augmentées » dans les espaces publics : la position de la CNIL », disponible sur www.cnil.fr, 19 juillet 2022.
[2] LA QUADRATURE DU NET, « Les dangers de la vidéosurveillance algorithmique (VSA) », disponible sur www.youtube.com, 15 mars 2023.
[3] CNIL, *op. cit*.
[4] *Ibidem.*
[5] *Ibidem.*

par des logiciels, permettant une analyse automatique, en temps réel et en continu, des images captées par la caméra »[6]. Ainsi, les termes de caméras « augmentées » utilisés par la CNIL désignent bel et bien la VSA. Il s'agit donc, selon elle, d'un dispositif qui diffère de la surveillance biométrique.

Pour la Quadrature du Net, il s'agit toutefois d'un outil de surveillance biométrique, « qui analyse les flux vidéos des caméras de vidéosurveillance afin d'alerter la police ou des agents de sécurité privés, lorsqu'elles détectent un élément qu'elles verraient comme suspect »[7].

Toujours selon l'association, nous serions face à « des logiciels qui analysent en permanence tous nos comportements dans la rue pour les classer comme étant normaux ou anormaux »[8].

Elle précise qu'aujourd'hui, « les flux vidéos des caméras de surveillance de l'espace public sont centralisés à l'échelle de communes, ou d'agglomérations de communes, dans des centres avec des écrans que l'on appelle des centres de supervision urbains (CSU) »[9]. Ces centres sont composés d'agents municipaux, qui surveillent les images et déclenchent une intervention policière lorsqu'ils pensent être témoins d'une activité délictuelle ou criminelle, en vue de multiplier les arrestations en flagrant délit[10].

La VSA, elle, « vise à automatiser le travail de ces agents, en utilisant des logiciels qui déclencheraient des alertes de manière automatique »[11].

L'association Technopolice, quant à elle, définit la VSA comme « l'ajout d'une couche d'algorithme aux caméras de vidéosurveillance dites « classiques » et ce, dans le but de rendre automatique l'analyse des images captées par caméras, jusqu'à présent réalisée par des humains, des opérateurs vidéo au sein de centres de supervision urbains (CSU)»[12].

La VSA doit donc être entendue, dans le cadre du présent travail, au sens d'une automatisation de l'analyse des flux vidéos des caméras de surveillance, par le biais d'algorithmes, afin d'alerter la police en temps réel de comportements dits « anormaux ». Nous aurons l'occasion de revenir sur cette notion, notamment sur la manière dont l'algorithme établit la distinction entre les comportements « normaux » et « anormaux » et sur ses conséquences.

§3. Fonctionnement de la vidéosurveillance algorithmique

Jusqu'à présent, nous avons retenu que les caméras « augmentées » ne sont autres que des caméras classiques, auxquelles l'on applique des algorithmes, qui vont permettre d'automatiser l'analyse des images captées par ces caméras. Cela, dans le but d'alerter la police le plus rapidement possible d'un comportement « anormal », puisque nous parlons ici de la VSA dans le cadre d'un objectif de sécurité.

---

[6] *Ibidem.*
[7] LA QUADRATURE DU NET, *op. cit.*
[8] *Ibidem.*
[9] *Ibidem.*
[10] *Ibidem.*
[11] *Ibidem.*; F. CASTAGNINO, 2019, « Rendre « intelligentes » les caméras : déplacement du travail des opérateurs de vidéosurveillance et redéfinition du soupçon », *Sciences Po*, n°5, 2019.
[12] ALOUETTE, « Qu'est-ce que la vidéosurveillance algorithmique ? », disponible sur www.technopolice.fr, 29 mars 2022. ; LA QUADRATURE DU NET, « Qu'est-ce que la vidéosurveillance algorithmique ? », disponible sur www.laquadrature.net, 23 mars 2022.

Mais *comment cela fonctionne-t-il concrètement ?* Il nous faut déjà savoir ce qu'est un algorithme en tant que tel. Un algorithme est « un ensemble de règles à suivre pour accomplir une tâche ou résoudre un problème »[13]. Il peut s'apparenter à une recette de cuisine[14] : une description des étapes à suivre pour atteindre un résultat donné.

Comme le souligne la professeure Elise DEGRAVE, « un algorithme, ce n'est pas une chose pure et vierge qui descend du ciel ! C'est une suite d'instructions mathématiques, décidées par un être humain : le concepteur d'algorithme. Forcément, ce concepteur d'algorithme programme en fonction de sa propre sensibilité. Le problème, c'est que son choix est intégré dans un outil utilisé à l'échelle de tout le pays. Du coup, ce choix technique individuel devient un choix de société ». Nous voyons d'ores et déjà que la conception de l'algorithme en lui-même peut mener à des choix politiques controversés.

Mais revenons à la VSA. Pour automatiser l'analyse des comportements humains dans les flux vidéo, les logiciels de VSA sont basés sur des algorithmes de **machine learning** (ou « apprentissage automatique »)[15]. Cela signifie qu'à partir de grandes bases de données de flux vidéos, des algorithmes apprennent « à repérer la présence d'objets et d'humains, leurs déplacements, leur vitesse, afin d'isoler certains événements catégorisés comme suspects. Ils provoquent ainsi une alerte pour mener à une intervention policière »[16].

A titre d'exemple, si nous voulons que l'algorithme puisse détecter qu'une personne est allongée, des milliers d'images de cette situation seront fournies à ce dernier afin qu'il établisse des corrélations entre toutes ces images, en vue de pouvoir détecter à nouveau cette situation dans de nouvelles images[17].

Pour cela, il prend en compte toute information utile. C'est précisément à ce stade que la controverse sur la définition de la VSA prend place puisque selon la Quadrature du Net, l'algorithme tient compte de toute information, même si elle est sensible et révèle par exemple une orientation politique, sexuelle ou religieuse[18].

Elle se justifie en reprenant l'exemple de la détection d'une personne qui serait allongée. Dans ce cas, « l'algorithme pourra utiliser comme données aussi bien la couleur des vêtements ou la taille de la personne que les informations qui ne sont pas perceptibles pour des humains »[19].

En effet, les algorithmes sont basés sur le **deep learning**. Il s'agit d'une « technique de machine learning reposant sur le modèle des réseaux neurones: des dizaines voire des centaines de couches de neurones sont empilées pour apporter une plus grande complexité à l'établissement des règles »[20]. L'idée est de pouvoir s'accommoder de grands volumes de données. Il s'agit d'une technologie avec un degré de complexité élevé. Les différentes couches, et l'apprentissage automatique de l'algorithme, entrainent une opacité du fonctionnement de l'algorithme, même pour son concepteur. Ainsi, selon la Quadrature du Net, il ne serait

[13] X, « Algorithme : Qu'est-ce que c'est ? A quoi ça sert ? », disponible sur www.datascientest.com, 11 août 2021.
[14] CNIL, « Algorithme », disponible sur https://www.cnil.fr, *s.d.,* consulté le 2 mars 2023.
[15] LA QUADRATURE DU NET, « Les dangers de… », *op. cit.*
[16] *Ibidem.*
[17] *Ibidem.*
[18] *Ibidem.*
[19] *Ibidem.*
[20] X, « Deep Learning ou Apprentissage Profond : qu'est-ce que c'est ? », disponible sur www.datascientest.com, 28 septembre 2020.

donc « pas possible techniquement de faire en sorte de protéger les données les plus sensibles et de les exclure du traitement »[21].

SECTION 2. CADRE LÉGAL EUROPÉEN

A présent que nous savons ce qu'est la VSA et comment elle fonctionne, nous pouvons comprendre qu'il est important d'encadrer juridiquement cette technologie. En effet, pour analyser et interpréter des flux vidéos, comme nous l'avons souligné, la VSA doit avoir accès à des données à caractère personnel. Dans certains cas, il pourra même s'agir de données sensibles, si l'on considère que la VSA est une forme de surveillance biométrique.

§1. Application du règlement général sur la protection des données (RGPD) à la vidéosurveillance algorithmique

Pour rappel, une donnée est considérée comme étant à caractère personnel dès lors qu'il s'agit d'une information « se rapportant à une personne physique identifiée ou identifiable »[22]. Les données sensibles, quant à elles, sont des données à caractère personnel qui ne peuvent, en principe, pas être traitées[23]. Il s'agit, par exemple, de données relatives à des convictions religieuses, à des données génétiques ou encore à des **données biométriques**.

En analysant nos émotions et nos comportements, la VSA traite bel et bien de données à caractère personnel. Qui plus est, il peut s'agir de données sensibles qui méritent alors une protection spécifique, puisqu'elles sont « par nature particulièrement sensibles du point de vue des libertés et des droits fondamentaux »[24]. Ainsi, le règlement général sur la protection des données (ci-après « RGPD ») tend à s'appliquer à la VSA.

La Directive (UE) 2016/680 du 27 avril 2016, qui protège les personnes physiques du traitement de leurs données à caractère personnel par les autorités compétentes à des fins de prévention[25], est également d'application.

En ce qui concerne la vidéosurveillance, les principes du RGPD doivent être respectés par les responsables du traitement. Sans les développer, il convient d'accorder une attention particulière aux principes suivants : licéité du traitement[26], finalité du traitement[27], minimisation des données[28], qualité et exactitude des données[29], conservation limitée des

[21] LA QUADRATURE DU NET, « Les dangers de… », *op. cit.*
[22] 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), art. 4, 1), *J.O.U.E.,* L 119/1, 4 mai 2016. (ci-après abrégé « RGPD »).
[23] Art. 9 RGPD.
[24] Considérant 51 RGPD.
[25] 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 119/89, 4 mai 2016.
[26] Art. 6 RGPD.
[27] Art. 5, §1, b) RGPD.
[28] Art. 5, §1, c) RGPD.
[29] Art. 5, §1, d) RGPD.

données[30], protection particulière des données sensibles[31], obligation d'intégrité et confidentialité (sécurité)[32], transparence[33], droit des personnes (information, accès, rectification,…)[34], et protection des données dès la conception et protection des données par défaut[35].

Il s'agit là des grands principes du RGPD qu'il convient de respecter lorsque des données à caractère personnel sont traitées. Nous noterons également que l'article 22 du règlement peut également être utile en matière de VSA puisqu'il instaure le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé[36]. Cette disposition souligne l'importance d'avoir un contrôle humain, même si elle prévoit des exceptions au principe.

Compte tenu de l'importance de ces règles pour l'encadrement de la VSA, nous nous pencherons sur l'implantation de ces principes de base en Europe, en nous intéressant particulièrement à la France et à la Belgique.

§2. Proposition de loi européenne sur l'intelligence artificielle (Artificial Intelligence Act)

Dans la lignée du règlement général sur la protection des données, le Parlement européen a adopté, le 14 juin 2023, le texte de proposition de la loi sur l'intelligence artificielle (ci-après « AI Act » pour *Artificial Intelligence Act)*. La réglementation avait été présentée par la Commission européenne en avril 2021, afin de poser le premier cadre réglementaire de l'Union européenne pour l'intelligence artificielle (ci-après « IA »). Il s'agit de la première loi globale sur l'IA au monde[37].

Si cette proposition est née, cela est dû à la « rapidité des évolutions technologiques et des éventuels défis à relever à cet égard »[38]. De fait, si l'intelligence artificielle peut procurer de nombreux avantages économiques et sociaux, elle peut également « être à l'origine de nouveaux risques ou de conséquences négatives pour les personnes ou la société »[39]. C'est pourquoi l'Union européenne a décidé d'adopter une approche dite équilibrée entre une évolution technologique nécessaire et la protection des droits fondamentaux. L'objectif est donc de « placer l'Europe en tête de la course à l'innovation, tout en garantissant la sécurité et les droits des utilisateurs »[40].

Ainsi, c'est « dans le cadre de sa stratégie numérique que l'UE souhaite réglementer l'intelligence artificielle (IA) pour garantir de meilleures conditions de développement et d'utilisation de cette technologie innovante »[41].

---

[30] Art. 5, §1, e) RGPD.
[31] Art. 9 RGPD.
[32] Art. 5, §1, f) RGPD.
[33] Art. 5, §1, a) RGPD.
[34] Art. 13 à 22 RGPD.
[35] Art. 25 RGPD.
[36] Art. 22 RGPD.
[37] X, « Loi sur l'IA de l'UE : première réglementation de l'intelligence artificielle », disponible sur www.europarl.europa.eu, 9 juin 2023, mis à jour le 14 juin 2023.
[38] 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. (ci-après abrégé « AI Act »).
[39] *Ibidem.*
[40] REUTERS, AFP et L. RENSON, « Qu'est-ce que l' « AI Act », la législation sur l'intelligence artificielle de la Commission européenne? », disponible sur www.lecho.be, 22 mars 2023.
[41] X, « Loi sur l'IA de l'UE… », *op. cit.*

Dans sa proposition, la Commission préconise une « approche par les risques »[42]. En effet, la stratégie adoptée consiste à analyser et classer les systèmes d'IA en fonction de leur niveau de risque pour les utilisateurs, allant de « faible » à « inacceptable ». Concrètement, différentes règles devront être respectées en fonction du niveau de risque que présente le système d'IA.

Actuellement, « la priorité du Parlement est de veiller à ce que les systèmes d'IA utilisés dans l'UE soient sûrs, transparents, traçables, non discriminatoires et respectueux de l'environnement. Les systèmes d'IA devraient également être supervisés par des personnes plutôt que par l'automatisation, afin d'éviter des résultats néfastes »[43]. Un parallèle peut être fait avec l'article 22 du RGPD, qui accorde le droit de ne pas faire l'objet d'une décision entièrement automatisée. La présence d'un humain pour contrôler l'IA paraît primordiale pour éviter les dérives.

Ensuite, il est à noter que si nous avons souligner la difficulté de définir la VSA, le Parlement souhaite également « établir une définition uniforme et neutre sur le plan technologique de l'IA qui pourrait être appliquée aux futurs systèmes d'IA »[44]. Nous verrons notamment que la définition donnée à un « système d'identification biométrique à distance en temps réel » aura des conséquences sur le plan juridique.

Pour en venir à l'AI Act en lui-même, passons en revue les différents types de risques et ce qu'ils impliquent comme obligations. Il existe trois types de risques.

1. Risque inacceptable

Tout d'abord, l'AI Act interdit les systèmes d'IA qui sont considérés comme une menace pour les personnes[45]. Ces pratiques interdites comprennent[46] :

- « la manipulation cognitivo-comportementale de personnes ou de groupes vulnérables spécifiques : par exemple, des jouets activés par la voix qui encouragent les comportements dangereux chez les enfants.

- un score social : classer les personnes en fonction de leur comportement, de leur statut socio-économique, de leurs caractéristiques personnelles.

- des systèmes d'identification biométrique en temps réel et à distance, tels que la reconnaissance faciale »[47].

Toutefois, il est à noter que certaines exceptions existent, notamment pour l'identification biométrique, par exemple si son utilisation est strictement nécessaire « pour la recherche ciblée de victimes potentielles spécifiques de la criminalité, notamment d'enfants disparus »[48], ou encore pour la prévention d'une attaque terroriste[49].

---

[42] O. MAQUINDUS, « « AI Act » : comment l'UE investit déjà dans des intelligences artificielles à « haut risque » pour contrôler ses frontières », disponible sur www.lemonde.fr, 22 juin 2023.
[43] X, « Loi sur l'IA de l'UE… », *op. cit.*
[44] *Ibidem.*
[45] *Ibidem.*
[46] Art. 5 AI Act.
[47] X, « Loi sur l'IA de l'UE… », *op. cit.*
[48] Art. 5, §1, d), i) AI Act.
[49] Art. 5, §1, d), ii) AI Act.

Pour l'application de ces exceptions, il faudra notamment tenir compte :

- « De la nature de la situation donnant lieu à un éventuel recours au système, en particulier la gravité, la probabilité et l'ampleur du préjudice causé en l'absence d'utilisation du système;

- Des conséquences de l'utilisation du système sur les droits et libertés de toutes les personnes concernées, notamment la gravité, la probabilité et l'ampleur de ces conséquences »[50].

Cette utilisation fera également l'objet d'une autorisation préalable octroyée par une autorité judiciaire ou une autorité administrative indépendante de l'État membre dans lequel cette utilisation doit avoir lieu, délivrée sur demande motivée »[51].

Pour savoir si la VSA est considérée comme présentant un risque inacceptable, il convient de se pencher sur la définition d'un système d'identification biométrique à distance en temps réel. Selon la proposition, il s'agit d'un « système d'identification biométrique à distance dans lequel l'acquisition des **données biométriques,** la comparaison et l'identification se déroulent sans décalage temporel significatif »[52].

Les données biométriques, quant à elle, sont redéfinies comme étant « des données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou **comportementales** d'une personne physique, qui permettent ou confirment son **identification unique**, telles que des images faciales ou des données dactyloscopiques »[53].

Ainsi, si la VSA analyse le comportement des personnes, encore faut-il qu'elle identifie de manière unique un individu pour être classée parmi les systèmes d'IA inacceptables.

2. Risque élevé

Lorsque des systèmes impactent l'exercice des droits et libertés des individus, ils sont considérés comme étant à haut risque. Cela implique pour leurs développeurs « de respecter certaines exigences de qualité des données d'entrainement, de transparence, et un cadre qui permet une supervision humaine et une responsabilité suffisante. Désormais les autorités qui feront l'usage d'IA à haut risque devront effectuer et publier une analyse d'impact au regard des droits fondamentaux avant de les déployer »[54].

Ces systèmes d'IA à haut risque « seront divisés en deux catégories :

1. Les systèmes d'IA qui sont utilisés dans les produits relevant de la législation de l'UE sur la sécurité des produits. Cela comprend les jouets, l'aviation, les voitures, les dispositifs médicaux et les ascenseurs.

[50] Art. 5, §2, a) et b) AI Act.
[51] Art. 5, §3 AI Act.
[52] Art. 3, 37) AI Act.
[53] Art. 3, 33) AI Act.
[54] E. DEGRAVE, C. MAERTENS et L. ROY, « Les droits fondamentaux face aux algorithmes du secteur public », *Dossier Libertés Publiques*, 2023, p. 15 à 17. ; Art. 8, 9, 13 et 14 AI Act.

2. Les systèmes d'IA relevant de huit domaines spécifiques qui devront être enregistrés dans une base de données de l'UE :

   - l'identification biométrique et la catégorisation des personnes physiques
   - la gestion et l'exploitation des infrastructures critiques
   - l'éducation et la formation professionnelle
   - l'emploi, la gestion des travailleurs et l'accès au travail indépendant
   - l'accès et la jouissance des services privés essentiels et des services et avantages publics
   - les **forces de l'ordre**
   - la gestion de la migration, de l'asile et du contrôle des frontières
   - l'aide à l'interprétation juridique et à l'application de la loi »[55].

Dès lors, si la VSA ne répondait pas à la définition des risques inacceptables, elle se retrouverait néanmoins dans les risques élevés et devrait respecter certaines exigences, puisque « tous les systèmes d'IA à haut risque seront évalués avant leur mise sur le marché et tout au long de leur cycle de vie »[56].

3. Risque limité

Pour les systèmes d'IA présentant un risque limité, les fournisseurs doivent simplement « veiller à ce qu'ils soient conçus et développés de manière à ce que les personnes physiques soient informées qu'elles interagissent avec un système d'IA »[57], laissant ainsi le choix à l'utilisateur d'utiliser ou non l'IA. Concrètement, « cela inclut les systèmes d'IA qui génèrent ou manipulent du contenu image, audio ou vidéo (par exemple, les deepfakes, des contenus faux qui sont rendus crédibles par l'IA) »[58].

Voilà donc ce que prévoit la première loi au monde sur l'intelligence artificielle. En ce qui concerne son application, l'objectif est de parvenir à un accord sur la forme finale de la loi d'ici la fin de l'année[59]. Malheureusement, son application étant prévue pour 2025[60], ce texte ne verra pas le jour avant la mise en œuvre de la VSA lors des Jeux Olympiques et Paralympiques (JO) 2024 à Paris, un projet au cœur de l'actualité.

[55] X, « Loi sur l'IA de l'UE… », *op. cit.*
[56] *Ibidem.*
[57] Art. 52, §1 AI Act.
[58] X, « Loi sur l'IA de l'UE… », *op. cit.*
[59] *Ibidem.*
[60] P. LE CŒUR, « JO 2024 : les députés autorisent la vidéosurveillance algorithmique avant, pendant et après les Jeux », disponible sur www.lemonde.fr, 23 mars 2023, mis à jour le 18 avril 2023.

SECTION 3. EXEMPLES D'UTILISATION DE LA VIDÉOSURVEILANCE ALGORITHMIQUE

A présent, nous savons ce qu'est la VSA et ce qui est prévu au niveau européen pour son encadrement. Penchons-nous dès lors sur des exemples d'utilisation de la VSA au sein des États membres, en commençant par le cas français (*§1*) pour poursuivre avec la Belgique (*§2*).

§1. Illustration n°1 : la France

A. Le cadre légal français

En premier lieu, nous allons nous intéresser au cas de la France, mise en lumière ces derniers mois pour son projet de surveillance algorithmique aux prochains JO. Examinons tout d'abord le cadre légal applicable en la matière.

Pour ce faire, nous nous appuierons sur un document publié par la CNIL, concernant sa position sur les conditions de déploiement des dispositifs de vidéo « augmentée » dans les lieux ouverts au public[61]. Document dans lequel elle établit un rappel du cadre juridique applicable actuellement en France en matière de caméra « intelligente ».

En France, le cadre applicable à la vidéosurveillance traditionnelle est fixé par les articles L. 251-1 à L. 255-1 du **code de la sécurité intérieure** (ci-après « CSI »). Ces dispositions sont issues de la loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité[62].

Ainsi, nous observons qu'aucune disposition de ce code n'encadre les conditions de mise en œuvre des dispositifs de vidéo « augmentée ». Néanmoins, selon la CNIL, cela ne signifie pas que ces dernières doivent être considérées comme étant illicites par principe[63]. Mais selon elle, « il ne faut pas en déduire non plus que les caméras encadrées par le CSI seraient *de facto* autorisées à utiliser des technologies de vidéo « augmentée » y compris pour les finalités ayant permis leur implantation : le législateur n'a entendu encadrer par le CSI que des dispositifs de vidéo « simples », qui ne captent pas le son et ne sont pas équipés de traitements algorithmiques d'analyse automatique. Ainsi, l'analyse de la licéité des traitements algorithmiques sur lesquels repose la vidéo « augmentée » doit donc s'effectuer au cas par cas »[64].

Dès lors, notre premier constat est qu'il n'existe pas de cadre juridique spécifique pour la VSA en France, l'analyse au cas par cas venant renforcer cette insécurité juridique. Or, lorsque nous nous pencherons sur le projet relatif aux JO 2024, nous constaterons toutefois que le projet de loi, ainsi que le Conseil d'État français, sont plutôt d'avis qu'il faille procéder à « une mise en conformité des dispositions du code de la sécurité intérieure, issues de la loi 21 janvier 1995, aux exigences du droit des données personnelles en vigueur »[65]. Une approche au cas par cas n'est donc pas envisagée, au bénéfice d'une plus grande sécurité juridique. Lorsque l'AI Act

[61] CNIL, « Position sur les conditions de déploiement de caméras dites « intelligentes » ou « augmentées » dans les espaces publics », disponible sur www.cnil.fr, juillet 2022.
[62] Loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité, NOR : INTX9400063L, *JORF* n°0020, 24 janvier 1995.
[63] *Ibidem,* p. 11
[64] *Ibidem*, p. 11
[65] C.E., Avis sur un projet de loi relatif aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions, NOR : SPOX2233026L, *Assemblée générale*, n°406383, séance du 15 décembre 2022.

sera adopté, une harmonisation opérera également au niveau européen. Il conviendra alors de veiller à ce que la nouvelle loi française respecte les nouveaux principes en vigueur.

Cependant, « les images issues de la vidéosurveillance constituent des traitements de données à caractère personnel au sens du RGPD et de la Directive (UE) 2016/680 du 27 avril 2016, que la loi n° 78-17 du 6 janvier 1978 adapte et transpose en droit national »[66]. Ainsi, la France n'est pas dépourvue de protection en matière de vie privée, puisqu'il s'agit là d'une question harmonisée au niveau européen. Nous l'avons souligné, le **RGPD** tend à s'appliquer à la VSA au sein des États membres. En France, sa transposition se trouve au sein de la **loi Informatique et Libertés**[67]. Par conséquent, dès lors qu'un traitement de données à caractère personnel est effectué, ces deux réglementations devront être respectées.

Concrètement, cela implique que « les utilisateurs de ces solutions, et leurs concepteurs (sociétés qui développent et commercialisent ces dispositifs) devront, en fonction de leur qualification (responsable ou co-responsables du traitement ou sous-traitant), respecter les principes et garanties applicables en matière de protection des données à caractère personnel, que le dispositif soit déployé à titre expérimental ou non »[68].

A cet effet, la CNIL rappelle les grands principes qui devront alors faire l'objet d'une attention particulière :

- **Des finalités déterminées, explicites et légitimes** (art. 5.1.b RGPD). A cet égard, le Comité européen pour la protection des données (CEPD) rappelle également, dans ses lignes directrices portant sur les traitements de données à caractère personnel dans le cadre des systèmes de vidéosurveillance[69], l'importance de respecter les principes généraux du RGPD, énoncés en son article 5.

- **Une base légale appropriée** (art. 6 RGPD). Elle souligne que l'intérêt légitime[70] du responsable de traitement pourrait ne pas toujours être mobilisable comme base de licéité, notamment lorsque la mise en place des dispositifs de VSA conduirait à un « déséquilibre manifeste entre les droits et libertés des personnes et les intérêts du responsable du traitement »[71].

- **La nécessité et la proportionnalité du dispositif.** Nous reviendrons sur cette question ultérieurement.

- **Réalisation d'une analyse d'impact relative à la protection des données (AIPD)** (art. 35 RGPP) **et désignation éventuelle d'un délégué à la protection des données (DPD/DPO)** (art. 37 RGPD). En effet, une AIPD doit être réalisée « en raison du caractère innovant de cette technologie, tandis qu'un DPD/DPO devra être obligatoirement désigné pour les organismes (utilisateurs ou développeurs de ces solutions) dont les « activités de base » utilisent ces dispositifs à grande échelle »[72].

---

[66] *Ibidem.*
[67] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, *JORF*, 7 janvier 1978.
[68] C.E., *op. cit.*, p. 12.
[69] EDPB, « Lignes directrices 3/2019 sur le traitement des données à caractère personnel par des dispositifs vidéo », Version 2.0., disponible sur www.edpb.europa.eu, 29 janvier 2020.
[70] Art. 6, §1, f) RGPD.
[71] C.E., *op. cit.*, p. 12.
[72] *Ibidem*, p. 14.

- **La nécessaire information des personnes concernées** (art. 14 RGPD). Si tous les droits des personnes concernées doivent être respectés, une attention toute particulière doit être portée sur le droit à l'information des personnes. Il s'agit, selon la CNIL, d'un « élément essentiel pour assurer la loyauté du traitement »[73]. Concrètement, « une simple mise à jour des panneaux d'affichage d'un système de vidéoprotection, tels qu'on peut aujourd'hui les trouver dans les lieux publics, ne saurait a priori suffire. Il sera essentiel de porter à la connaissance des personnes concernées l'information clef du dispositif, qui réside dans le caractère « augmenté » des caméras, et également d'expliquer les caractéristiques et la portée d'une telle analyse. La fourniture de cette information sur des supports adaptés (panneaux d'information dédiés, vidéos, codes QR, marquages au sol, annonces sonores, etc.) est encouragée »[74].

Dans la même lignée, la CNIL souligne le fait que « la mise en œuvre des dispositifs de vidéo « augmentée » se heurte souvent, dans la pratique, à l'obligation de prendre en compte et de respecter de manière effective le **droit d'opposition** des personnes concernées »[75]. Cela est dû notamment au fonctionnement même de cette technologie, qui captent automatiquement des images et les analyse instantanément, en temps réel. Or, le droit d'opposition est normalement garanti par le RGPD et se doit d'être effectif et applicable à tout moment[76].

C'est pourquoi, il est important que les dispositifs de vidéo « augmentée » soient, sous réserve de ne pas pouvoir justifier de la mise en œuvre effective et acceptable d'un droit d'opposition, autorisés par un cadre légal spécifique de nature a minima réglementaire, conforme aux conditions posées par **l'article 23 du RGPD** »[77]. Le cadre réglementaire permettra dès lors de justifier « la légitimité et la proportionnalité du traitement opéré au regard de l'objectif poursuivi », mais également d'expliquer pourquoi il est nécessaire d'exclure la faculté pour les personnes concernées de s'y opposer. Il conviendra, dans ce cas, de fixer des garanties appropriées au bénéfice de ces dernières[78].

Enfin, cette obligation d'établir un cadre spécifique pour la VSA se voit confirmer par **l'article 34 de la Constitution française**. En effet, à partir du moment où certains dispositifs de caméras de vidéosurveillance peuvent être attentatoires aux libertés fondamentales du citoyen, il convient, si nous suivons la jurisprudence du Conseil d'État français en matière de caméras piétons et de drones[79], de considérer qu'il s'agit de questions qui relèvent des domaines constitutionnellement réservés à la loi[80].

---

[73] *Ibidem*, p. 14.
[74] *Ibidem*, p. 14.
[75] *Ibidem*, p. 14.
[76] Art. 21 RGPD.
[77] C.E., *op. cit.*, p. 15.
[78] *Ibidem*, p. 15.
[79] Pour les caméras piétons : INT – 390313, 23/09/2015 (cf. le rapport annuel du CE de 2015, p. 322-323 (PDF, 2,8 Mo) sur vie-publique.fr), puis position réitérée à l'occasion de son avis sur le projet de loi renforçant la lutte contre le crime organisé et son financement, l'efficacité et les garanties de la procédure pénale (sur conseil-etat.fr) ; le rapport annuel de la CNIL (PDF, 1,9 Mo) en 2016 fait le bilan de toutes ces étapes (p. 19 et 20) ; pour les drones : « Conseil d'État, section de l'intérieur, séance du mardi 20 septembre 2020 N° 401 21 », avis rendu au Gouvernement relatif à l'usage de dispositifs aéroportés de captation d'images par les autorités publiques.
[80] Const, art. 34.

B. Projet de loi relatif aux Jeux Olympiques et Paralympiques 2024

« Ouvrons grand les Jeux ». Il s'agit là du slogan choisi par le comité d'organisation français pour les Jeux Olympiques et Paralympiques 2024, qui se dérouleront à Paris.

Si les Jeux suscitent l'enthousiasme, ils sont également au cœur de nombreuses controverses. De fait, cet événement populaire a amené le gouvernement français à adopter plusieurs mesures, notamment en matière de sécurité, qui ne sont pas au goût de tous.

En cause, le projet de loi relatif aux Jeux Olympiques et Paralympiques de 2024, présenté au Conseil des ministres le 22 décembre 2022 par Amélie OUDÉA-CASTÉRA, ministre des sports et des Jeux Olympiques et Paralympiques[81].

Plus particulièrement, c'est l'article 7 de ce projet qui fait couler beaucoup d'encre. De fait, la fameuse disposition prévoit qu'à titre expérimental et jusqu'au 31 décembre 2024, des dispositifs de VSA seront utilisées afin d'assurer la sécurité des « manifestations sportives, récréatives ou culturelles »[82], en repérant des « événements » dont la liste sera définie par décret, après avis de la CNIL[83]. Cette mesure se fonde sur l'article L. 252-1 du CSI. Elle aura pour objectif de « détecter, en temps réel, des événements prédéterminés susceptibles de présenter ou de révéler ces risques et de les signaler en vue de la mise en œuvre des mesures nécessaires par les services de la police nationale et de la gendarmerie nationale, les services d'incendie et de secours, les services de police municipale et les services internes de sécurité de la SNCF et de la Régie autonome des transports parisiens dans le cadre de leurs missions respectives »[84].

Il est à noter que cette technologie ne concernera pas que les JO puisqu'elle s'appliquera également – à titre d'exemple - à la Coupe du monde de rugby cet automne, et qu'elle s'étendra au-delà des Jeux[85], jusqu'à la fin du mois de décembre 2024[86].

Ainsi, l'article 7 est sans doute le plus controversé du projet de loi, inquiétant principalement la gauche et les organisations de défense des droits de l'Homme[87]. Pourtant, la disposition a bel et bien été adoptée, le 23 mars 2023, à 59 voix contre 14[88]. Mais « les députés de la Nupes, qui ont été les seuls à voter contre cet article, s'inquiètent que le dispositif soit généralisé par la suite à la population »[89].

---

[81] X, « Loi du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions », disponible sur www.vie-publique.fr, 22 mai 2023.
[82] Projet de loi adopté par le Sénat, relatif aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions, art. 7, *Assemblée Nationale*, seizième législature, 1er février 2023, n°809. (ci-après abrégé « Projet de loi JO »).
[83] X, « Sécurité à Paris 2024 : inimaginable « de voir arriver un texte comme ça en France », s'insurgent des députés », disponible sur www.midilibre.fr, 20 mars 2023.
[84] Art. 7 Projet de loi JO.
[85] Pour information, les Jeux Olympiques et Paralympiques prochains auront lieu du 26 juillet au 8 septembre 2024 (C.E., *op. cit.*, p. 1).
[86] P. LE CŒUR, *op. cit.*
[87] R. HOUEIX, « Paris-2024 : les JO, cheval de Troie de la vidéosurveillance algorithmique ? », disponible sur www.france24.com, 24 mars 2023.
[88] G. DOSDA et AFP, « Loi sur les JO de 2024 : l'Assemblée adopte un article controversé sur la vidéosurveillance », disponible sur www.lejdd.fr, 23 mars 2023.
[89] *Ibidem.*

L'adoption de ce projet de loi fait de la France le premier pays de l'Union européenne à encadrer la vidéosurveillance augmentée, ce qui n'a pas manqué de faire réagir certains eurodéputés. Certains estiment qu' « en poussant à l'adoption rapide d'une loi permettant l'analyse automatisée des signaux comportementaux humains en dépit du processus européen actuellement en cours, la France sape le rôle de démocratie et de contrôle du Parlement européen »[90]. Ils craignent que l'article 7 n'entre en conflit avec la loi européenne sur l'IA.

Toutefois, rappelons-nous que l'AI Act tend à interdire « les systèmes d'identification biométrique à distance en temps réel ». Or, le ministre de l'Intérieur, Gérald DARMANIN, a affirmé qu'il ne serait pas question de reconnaissance faciale et de traitement biométrique[91]. Il s'agit, selon lui, d'une mesure nécessaire pour la sécurité des JO, durant lesquels pas moins de 13 millions de spectateurs seraient attendus[92]. La mise en place de la vidéosurveillance intelligente permettrait d'« éviter des incidents comme ceux qui ont eu lieu au Stade de France lors de la finale de la ligue des champions en mai 2022 »[93].

Le ministre insiste également sur le fait que « les événements prédéterminés concernent non pas des personnes mais des situations »[94]. Il donne alors quelques exemples d'évènements qui seront fixés par décret : « un départ de feu, des goulots d'étranglement de population, un colis ou un sac abandonné »[95]. Il conviendra dès lors de procéder à une analyse de conformité avec l'AI Act lorsque ce dernier sera en vigueur.

Mais malgré les explications du ministre de l'Intérieur, les groupes de gauche de la Nupes et des députés du groupe indépendant LIOT « ne sont pas convaincus et ont tenté sans succès d'obtenir la suppression ou la réécriture de l'article autorisant les traitements des images par des algorithmes »[96]. À titre d'illustration, Sandra REGOM, députée écologiste, estime que cette loi « propose de transformer en cobayes l'intégralité de la population sur le territoire français »[97]. A cet égard, elle a déclaré : « vous vous cachez derrière l'argument que la reconnaissance faciale sera interdite pour cacher le fait que les données sur les visages seront traitées par les algorithmes et archivées »[98].

Nonobstant les contestations de certains parlementaires, l'article 7 fit son chemin pour finir par être inscrit, en tant qu'article 10, dans la loi n° 2023-380, promulguée le 19 mai 2023[99]. Une modification a par ailleurs été apportée à ce nouvel article 10, qui prolonge désormais la période d'expérimentation jusqu'au 31 mars 2025, renforçant les craintes des parlementaires déjà sceptiques.

C'est ainsi que le 17 mai 2023, un recours fut introduit devant le Conseil constitutionnel par plusieurs députés, estimant notamment que « la durée de cette expérimentation serait excessive au motif qu'elle est prévue jusqu'au 31 mars 2025 alors qu'elle serait destinée à s'appliquer

---

[90] S. ROZENFELD, « Vidéosurveillance algorithmique : le précédent français », *Expertises*, n°489, 2023, p. 112.
[91] X, « JO 2024 : interdiction de la « reconnaissance faciale et du traitement biométrique », assure Darmanin, la gauche sceptique », disponible sur www.midilibre.fr, 23 mars 2023.
[92] *Ibidem.*
[93] X, « Loi du 19 mai 2023… », *op. cit.*
[94] G. DOSDA et AFP, *op. cit.*
[95] *Ibidem.*
[96] X, « JO 2024 : interdiction de la « reconnaissance faciale… », *op. cit.*
[97] *Ibidem.*
[98] *Ibidem.*
[99] Loi n° 2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions, NOR : SPOX2233026L, *JORF* n°0116, 20 mai 2023. (ci-après abrégé « Loi JO »).

aux jeux olympiques et paralympiques qui s'achèveront en septembre 2024 »[100]. Dans sa décision, le Conseil constitutionnel avait pourtant jugé conformes les articles portant sur les caméras « augmentées »[101], en estimant notamment que « le législateur a précisément fixé la durée maximale de l'expérimentation qu'il a autorisée »[102].

Enfin, il est à noter que l'article 10 de la loi exclut explicitement les traitements de données biométriques, éclaircissant ainsi le cadre juridique applicable à cet outil[103]. La vidéosurveillance augmentée utilisée lors des JO 2024 ne sera donc pas soumise au cadre juridique applicable aux données sensibles. Toutefois, les dispositions nationales et européennes en matière de données à caractère personnel devront être respectées, « dans la mesure où les dispositifs de vidéoprotection augmentée captent et analysent des données à caractère personnel »[104].

Nous verrons notamment, lorsque nous nous intéresserons aux dangers que peuvent présenter ces dispositifs de vidéosurveillance pour nos libertés fondamentales, que plusieurs garanties sont prévues par la nouvelle loi française.

§2. Illustration n°2 : la Belgique

A. Le cadre légal belge

En deuxième lieu, intéressons-nous à présent au cadre légal belge. Depuis 2007, la « loi caméras »[105] réglemente l'usage de la vidéosurveillance « afin d'assurer qu'elle n'empiète pas de façon excessive sur la vie privée des citoyens »[106]. Cette loi étant entrée en vigueur avant l'arrivée du RGPD, quelques modifications furent apportées par la loi du 21 mars 2018[107]. Nous ne les verrons pas toutes dans le cadre du présent travail, mais nous nous focaliserons plutôt sur la réglementation applicable à la VSA.

Il est à noter que cette loi modifie également la loi sur la fonction de police, qui autorise les services de police à faire usage de caméras dans le cadre de leur fonction, sous réserve de plusieurs conditions[108].

En ce qui concerne les caméras intelligentes, si elles ne sont pas reliées à des fichiers de données à caractère personnel (par exemple, les caméras qui détectent les mouvements), elles sont autorisées[109]. A l'inverse, si les caméras de surveillance intelligentes sont reliées à des fichiers de données à caractère personnel (reconnaissance des visages), elles ne sont pas autorisées. Une

[100] C.E., 17 mai 2023, n° 2023-850 DC, §27 .
[101] *Ibidem* ; X, « Loi du 19 mai 2023… », *op. cit.*
[102] *Ibidem,* §47.
[103] Art. 10, IV Loi JO.
[104] J. MAZILLIER, « RGPD : « caméras augmentées » sur le podium olympique : quelles garanties ? », Expertises, n°490, 2023, p. 176.
[105] Loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance, *M.B.*, 31 mai 2007. (ci-après abrégé « Loi caméras »).
[106] F. COTON, « Souriez, vous êtes filmé ! », disponible sur www.lexing.be, 17 mars 2023.
[107] Loi du 21 mars 2018 modifiant la loi sur la fonction de police, en vue de régler l'utilisation de caméras par les services de police, et modifiant la loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance, la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et la loi du 2 octobre 2017 réglementant la sécurité privée et particulière, *M.B.*, 16 avril 2018. (ci-après abrégé « Loi du 21 mars 2018 »).
[108] Loi du 5 août 1992 sur la fonction de police, *M.B.*, 22 décembre 1992, art. 25/1 à 25/8.
[109] X, « Caméras de surveillance – Nouvelle réglementation ! », disponible sur www.police.be, 12 juillet 2018.

exception est faite pour « la reconnaissance automatique des plaques d'immatriculation des véhicules par les administrations communales »[110].

En outre, « puisque les images où figurent des individus identifiables sont des données à caractère personnel, la « loi caméras » et le RGPD doivent fréquemment être appliqués en parallèle. Les principes régissant le traitement des données à caractère personnel doivent donc être respectés (proportionnalité, prise des mesures de sécurité nécessaires…) »[111]. En Belgique, le RGPD est transposé par la loi du 30 juillet 2018[112].

Cette coexistence entre le RGPD et la « loi caméras » implique également une coexistence des sanctions de ces deux réglementations. Ainsi, « les amendes administratives mises en place par le RGPD seront certainement plus appliquées, et donc plus dissuasives, que les sanctions pénales de la « loi caméras » »[113].

Enfin, outre la protection de la vie privée, il nous semble primordial d'évoquer la réglementation en matière de **transparence des algorithmes** du secteur public.

En septembre 2021, une loi avait été proposée afin d'introduire une plus grande transparence dans l'usage des algorithmes par l'administration[114]. Toutefois, « la transparence visée par le projet se limite à révéler le code source de l'algorithme »[115], ce qui peut laisser présager une information insuffisante pour la pleine compréhension du citoyen de l'algorithme, d'après l'Autorité de Protection des Données[116].

Deux ans plus tard, le 10 février 2023, « le Sénat a voté une intéressante proposition de résolution relative à la mise en place d'une autorité de contrôle des algorithmes[117]. Curieusement, cette initiative a fait peu de bruit autour d'elle, alors qu'elle est particulièrement intéressante dans le contexte actuel »[118].

Cela rejoint la conclusion de Lucie CLUZEL, Professeure à l'Université Paris-Nanterre, lors d'une conférence organisée par la Chaire Francqui, intitulée « *Vers un contrôle démocratique ?* ».[119] Elle soulignait qu'il serait intéressant de développer un contrôle démocratique. Une commission parlementaire pourrait être mise en place et serait alors dédiée à certaines utilisations problématiques de l'algorithme. Il pourrait en effet être intéressant que le Parlement se saisisse de ces questions, même si ce n'est pas un contrôle qui est envisagé pour l'instant. Cette idée pourrait être intéressante en ce qu'un contrôle humain, et qui plus est démocratique, est le plus souvent une solution souhaitable.

---

[110] Art. 26 Loi du 21 mars 2018. ; F. COTON, *op. cit.*
[111] *Ibidem.*
[112] Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, *M.B.*, 5 septembre 2018.
[113] F. COTON, *op. cit.*
[114] Proposition de loi modifiant la loi relative à la publicité de l'administration du 11 avril 1994 afin d'introduire une plus grande transparence dans l'usage des algorithmes par l'administration, *Doc.*, Ch., 55, 2020-2021, n°1904/001.
[115] E. DEGRAVE, C. MAERTENS et L. ROY, *op. cit.*, p. 17.
[116] Avis de l'Autorité de Protection des Données n° 157/2021 du 10 septembre 2021.
[117] Proposition de résolution relative à la mise en place d'une autorité de contrôle des algorithmes, *Ann. Parl.*, Sén., 2022-2023, séance du 10 février 2023, n°7-328/4.
[118] E. DEGRAVE, C. MAERTENS et L. ROY, *op. cit.*, p. 17.
[119] L. CLUZEL, Cours-Conférence donné dans le cadre de la Chaire Francqui en E-gouvernement de l'UNamur, 10 mars 2023.

Bien qu'il puisse être, en pratique, compliqué de trouver le moyen de superviser les algorithmes, un tel contrôle nous paraît primordial, de surcroît lorsqu'il est question de limiter nos droits fondamentaux.

Il s'agit là de la question dite de **l'opacité** de l'algorithme. Dans le cadre de la VSA, l'opacité résiderait dans le fait de savoir comment un comportement suspect est détecté : *qu'est-ce qu'un comportement suspect pour l'IA ?* Il s'agit alors de connaître non seulement le code source, mais également les éventuels biais du concepteur de l'algorithme. En effet, un algorithme est développé par des humains qui se devront de faire des choix lors de sa conception. Ces choix auront ensuite des conséquence sur l'interprétation que l'IA donnera ou non à certaines situations. Cela peut malheureusement mener à des situations de discriminations, sur lesquelles nous reviendrons ultérieurement.

Mais comme nous l'avons souligné, ce contrôle peut être difficile à mettre en œuvre, en ce que la VSA est une technologie tellement complexe que son concepteur lui-même ne peut parfois expliquer pourquoi l'IA choisit une interprétation plutôt qu'une autre. D'où le danger de se fier intégralement à l'intelligence artificielle, d'autant plus lorsqu'il s'agit d'une question de sécurité. Si la VSA peut être d'une aide précieuse aux services de police lors de grands événements, tels les JO, se fier entièrement à ce système en oubliant complètement les contrôles humains ne paraît dès lors pas être la solution. Nous serions plutôt d'avis que des agents contrôlent les alertes des dispositifs techniques – comme il est d'ailleurs prévu – mais que d'autres agents se chargent également de la surveillance des Jeux sans soutien d'une VSA, comme ils l'ont toujours fait. Cela doublerait ainsi les chances de détecter des comportements dits « anormaux ».

B. Utilisations de caméras « intelligentes » en Belgique

Ainsi, nous avons vu que la Belgique dispose d'un cadre légal permettant la protection de la vie privée des citoyens. Elle est également quelque peu avancée par rapport à la France, puisqu'elle se pose notamment des questions quant à un éventuel contrôle de l'algorithme. Les questions de transparence sont en effet d'une grande importance afin d'éviter les dérives.

En examinant le cadre légal belge, nous avons pu constater qu'aucune loi n'encadre l'usage des technologies de reconnaissance faciale par les autorités publiques. La reconnaissance faciale n'est pas totalement interdite, mais doit suivre les garanties établies par le RGPD, s'agissant de données sensibles.

Et pourtant, malgré l'absence d'un cadre l'autorisant, « la reconnaissance faciale a déjà été utilisée par la police belge à plusieurs reprises. En 2017 et en 2019, la reconnaissance faciale a été testée par la police fédérale à l'aéroport de Zaventem »[120], afin de « comparer des photos d'auteurs de crimes connus, en des endroits spécifiques, sur place et en temps réel »[121]. Cette méthode ne sortirait pas, selon Sarah FREDERICKX, porte-parole de la Police fédérale, du cadre de la loi sur la fonction de police qui autorise d'avoir recours à des dispositifs intelligents si

[120] X, « Pour l'interdiction de la reconnaissance faciale à Bruxelles », disponible sur www.mrax.be, 28 mars 2023. ; EDRI, « Protect My Face: Brussels residents join the fight against biometric mass surveillance », disponible sur https://edri.org, 29 mars 2023.
[121] L.H. et P.M., « La reconnaissance faciale est en test à Brussels Airport », disponible sur www.rtbf.be, 10 juillet 2019.

aucune conservation des informations récoltées n'est réalisée. Elle affirme qu'aucun stockage de données ne sera effectué et aucune base de données créée[122].

Ensuite, en 2019 et 2020, « la police fédérale a utilisé, à 78 reprises, Clearview AI, un logiciel controversé de reconnaissance faciale »[123]. Si cet outil est controversé c'est parce qu'il « alimente une base de données gigantesque en allant chercher des photos libres d'accès sur internet, sur les réseaux sociaux notamment. La base de données contient déjà plusieurs milliards de visages. Toutes ces données, croisées entre elles permettent au logiciel de mettre un nom sur un visage qui lui est présenté »[124].

Si les policiers belges ont eu recours à cet outil, c'était en vue de lutter contre les abus sexuels de mineurs, Clearview affirmant lui-même avoir joué un rôle dans l'identification de pédophiles par le passé[125]. Un objectif noble, certes, mais pour l'instant illégal car non prévu par la loi belge. En outre, il ne s'agissait pas uniquement d'utilisation de données à caractère personnel, mais également biométriques, ce qui implique que des garanties supplémentaires auraient dû être respectées. Ainsi, « l'Organe de contrôle de l'information policière a exigé la fin de ces expérimentations, aucun fondement juridique ne les autorisant »[126].

Cette expérimentation aura sans doute été au départ d'une réflexion de nos parlementaires belges, qui ne sont pas tous opposés à l'utilisation de telles technologies s'il existait un cadre légal en la matière. Selon le député PS, Hervé RIGOT, cette réglementation serait alors établie à l'issue d'un long débat parlementaire sur « la sécurité de ces logiciels, la protection de la vie privée, le respect de nos citoyens et sur le cadre »[127].

Cette dernière illustration nous permet de basculer vers la seconde partie de notre travail, qui consiste à nous interroger sur les limites du cadre actuel et les dérives qui sont justement liées à la VSA. Si un débat parlementaire devait avoir lieu – comme c'est d'ailleurs le cas au niveau européen actuellement – il s'agit de voir quelles questions il conviendrait de se poser, afin de trouver un juste équilibre entre sécurité et protection de nos droits fondamentaux.

[122] *Ibidem.*
[123] J-F. NOULET et D. BRICHARD, « L'utilisation du logiciel de reconnaissance faciale « Clearview » par les policiers belges était illégale », disponible sur www.rtbf.be, 9 mars 2022.
[124] *Ibidem.*
[125] *Ibidem.*
[126] X, « Pour l'interdiction de la reconnaissance faciale… », *op. cit.*
[127] J-F. NOULET et D. BRICHARD, *op. cit.*

TITRE II. Limites du cadre actuel : les possibles dérives liées à la vidéosurveillance algorithmique

SECTION 1. LES CAMÉRAS « INTELLIGENTES »: UNE MENACE POUR NOS LIBERTÉS FONDAMENTALES ?

Nous l'avons vu, l'article 7 du projet de loi concernant les prochains JO français a fait grand bruit. Et pour cause, des députés mais également de nombreuses associations se sont insurgés contre la fameuse disposition, considérant que « son adoption créerait un précédent inquiétant de surveillance injustifiée et disproportionnée dans les espaces accessibles au public, au détriment des droits et libertés fondamentaux »[128]. Mais *de quelles libertés est-il question et en quoi la VSA présente-t-elle une menace pour ces libertés ?* (*§1*). C'est ce que nous tenterons d'analyser, en nous interrogeant ensuite sur la nécessité et la proportionnalité de la mise en place d'un dispositif attentatoire à nos droits fondamentaux (*§2*).

§1. Les libertés fondamentales en cause

Il convient donc d'identifier en premier lieu quelles sont les libertés menacées par l'utilisation de telles technologies.

Dans une lettre de la société civile aux députés français sur le projet de loi relatif aux Jeux olympiques et paralympiques 2024, pas moins de 37 organisations mettent en garde sur le fait que cette disposition « représente une grave menace pour les libertés civiques et les principes démocratiques »[129].

Les organisations soulignent que la présence de dispositifs de vidéosurveillance algorithmique présente des risques inacceptables pour de nombreux droits fondamentaux, tels que le droit à la vie privée[130], le droit à la liberté de réunion et d'association[131], la liberté d'expression [132] et le droit à la non-discrimination[133].

Cette analyse est également partagée par la Professeure Lucie CLUZEL[134], qui estime qu'il existe certes un risque d'atteinte à la vie privée mais également à d'autres libertés. Le sentiment de surveillance instauré par de tels dispositifs « peut avoir un effet dissuasif sur les libertés civiques fondamentales »[135]. Si les citoyens se sentent surveillés, ils pourraient **s'autolimiter** par crainte de sanctions. Par exemple, l'utilisation de drones, en France, dans un but de prévention des troubles à l'ordre public, pourrait pousser les Français à ne pas aller dans les rues manifester, par peur d'une utilisation d'images en leur défaveur[136]. Plus concrètement, les

---

[128] Traduction libre de EDRI, *op. cit.*

[129] AMNESTY INTERNATIONAL *et al.*, « Lettre de la société civile aux députés français sur le projet de loi relatif aux Jeux olympiques et paralympiques 2024 », disponible sur www.edri.org, *s.d.*, consulté le 15 juin 2023, p. 1.

[130] Convention de sauvegarde des droits de l'homme et des libertés fondamentales, signée à Rome le 4 novembre 1950, approuvée par la loi du 13 mai 1955, *M.B.*, 19 août 1955, *err.*, 29 juin 1961, art. 8. (ci-après abrégé « Conv. E.D.H. ») ; Const., art. 22.

[131] Art. 11 Conv. E.D.H.; Const., art. 27.

[132] Art. 10 Conv. E.D.H.; Const., art.19 et 25.

[133] Art. 14 Conv. E.D.H.; Const., art. 10 et 11.

[134] L. CLUZEL, Cours-Conférence donné dans le cadre de la Chaire Francqui en E-gouvernement de l'UNamur, 16 février 2023.

[135] AMNESTY INTERNATIONAL *et al.*, *op. cit.,* p. 1.

[136] Loi du 24 janvier 2022 relative à la responsabilité pénale et à la sécurité intérieure, NOR : JUSX2116059L, *JORF*, 25 janvier 2022.

personnes présentes dans des espaces publics surveillés pourraient redouter d'être « identifiées, repérées ou même poursuivies à tort »[137].

Il s'agirait de la fin de l'anonymisation dans ces endroits surveillés, ce qui aurait dès lors un impact considérable sur l'exercice de nos libertés.

Si aucun cadre légal ne vient trouver un juste équilibre entre objectif de sécurité et sauvegarde de nos droits fondamentaux, l'usage de ces technologies constituerait un outil de rupture de l'égalité entre les citoyens, selon la Professeure CLUZEL.

La CNIL, quant à elle, insiste sur les risques nouveaux qu'entraîne la VSA pour le droit à la vie privée, notamment car l'exercice du droit d'opposition par les personnes concernées n'est pas possible dans de telles circonstances. Elle estime qu' « une généralisation non maîtrisée de ces dispositifs, par nature intrusifs, conduirait à un risque de surveillance et d'analyse généralisée dans l'espace public susceptible de modifier, en réaction, les comportements des personnes circulant dans la rue ou se rendant dans des magasins »[138]. Dans son avis relatif au déploiement de caméras « augmentées » dans les espaces publics, elle invite ainsi le législateur à prévoir un texte réglementaire ou législatif comme l'exige l'article 23 du RGPD dans ce cas, et à « éviter une multiplication disproportionnée de ces dispositifs, qui modifierait notre rapport à l'espace public »[139].

§2. Une mise en balance : les critères de nécessité et de proportionnalité

Ainsi, nous avons pu constater que l'implantation de cette technologie dans l'espace public pouvait représenter une véritable menace pour l'exercice de nos libertés. En particulier, c'est notre droit à la vie privée qui est menacé.

Toutefois, le RGPD lui-même insiste sur le fait qu'il ne s'agit pas d'un droit absolu. De fait, le considérant 4 du règlement dispose que « le droit à la protection des données à caractère personnel n'est pas un droit absolu; il doit être considéré par rapport à sa fonction dans la société et être mis en balance avec d'autres droits fondamentaux, conformément au principe de proportionnalité ». Il s'agit de la nécessité d'opérer une mise en balance « à chaque intégration de toute innovation au sein de la société »[140] .

A cet égard, la CNIL précise que « la démonstration, documentée par le responsable de traitement et adaptée à la base juridique retenue, de la **nécessité** et de la **proportionnalité** d'un dispositif de vidéo « augmentée » est essentielle avant tout déploiement de celui-ci »[141]. Elle rappelle également que « cette évaluation sera d'ailleurs nécessaire, selon les cas, dans le cadre de la réalisation de l'analyse d'impact relative à la protection des données (AIPD) qui devra être réalisée en amont pour une large majorité des cas d'usages des dispositifs de vidéo augmentée »[142].

---

[137] AMNESTY INTERNATIONAL *et al.*, *op. cit.*
[138] CNIL, « Déploiement de caméras « augmentées » dans les espaces publics : la CNIL publie sa position », disponible sur www.cnil.fr, 19 juillet 2022.
[139] *Ibidem.*
[140] J. MAZILLIER, *op. cit.*, p. 176.
[141] CNIL, « Position sur les conditions de déploiement de caméras… », *op. cit.*, p. 13.
[142] *Ibidem*.

En matière de protection de la vie privée, la CNIL établit un sommaire intéressant reprenant les principes à respecter en vertu du RGPD.

En premier lieu, elle commence par le critère de **nécessité,** en spécifiant tout d'abord que « pour la plupart des bases légales prévues par l'article 6 du RGPD, celui-ci exige que le traitement soit nécessaire à l'objectif poursuivi. Ainsi, la démonstration de la nécessité du traitement pourra notamment passer par l'évaluation :

- de **l'existence ou non de moyens moins intrusifs** permettant d'atteindre la finalité envisagée (par exemple : utilisation de capteurs infrarouges, de capteurs de véhicules sur la chaussée, de détecteur de présence, de capteurs de dispositifs électroniques utilisant les technologies Bluetooth ou Wi-Fi, réalisation d'enquêtes de fréquentation ou d'usage, recours à des vigiles, etc.) ;

- de l'utilité et de la **performance opérationnelle** du dispositif au regard de l'objectif poursuivi »[143].

En ce qui concerne le critère de performance opérationnelle du dispositif, certains estiment que la VSA n'a pas encore fait ses preuves. Rien ne prouverait l'efficacité d'une telle technologie, ni le fait que l'objectif de sécurité pourrait être accompli par le biais d'algorithmes[144].

A ce sujet, une étude française, menée par Guillaume GORMAND, chercheur au Centre d'études et de recherche sur la diplomatie, l'administration publique et le politique, a démontré l'inefficacité de la vidéosurveillance traditionnelle. En effet, elle met en lumière « un faible taux d'élucidation des infractions et des effets quasiment nuls en matière de prévention de la délinquance »[145]. Il reste à déterminer si cela signifie que la VSA serait quant à elle plus efficace, ou si au contraire, nous devons en déduire qu'une surveillance par caméra ne serait, de toute façon, pas dissuasive pour les auteurs d'infractions.

Ensuite, la CNIL rappelle que le principe de **minimisation des données** devra également être respecté, à savoir que seules seront prises en compte les données à caractère personnel qui sont « adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées »[146]. Concrètement, cela signifie que « les données traitées ne devront pas excéder ce qui est **nécessaire** pour atteindre les finalités envisagées »[147].

En deuxième lieu, la CNIL se penche sur le critère de **proportionnalité.** Concernant ce second critère, « le responsable de traitement doit, dans tous les cas, s'assurer que son traitement ne conduit pas à porter une atteinte disproportionnée à la protection qui doit être garantie à la vie privée et aux données à caractère personnel des personnes physiques. La proportionnalité d'un dispositif repose notamment sur les garanties qu'il met en œuvre. À ce titre, les mécanismes effectifs de protection de la vie privée dès la conception (« ***privacy by design*** »)[148] doivent être mis en œuvre pour réduire les risques pour les personnes concernées »[149]. Cela vise notamment

[143] *Ibidem*, p. 13
[144] D. LELOUP, « Adoptée pour les JO de Paris 2024, la surveillance algorithmique n'a jamais fait ses preuves », disponible sur www.lepolitique.net, 10 mars 2023.
[145] A. ALBERTINI, « Une étude commandée par les gendarmes montre la relative inefficacité de la vidéosurveillance », disponible sur www.lemonde.fr, 22 décembre 2021.
[146] Article 5, §1, c) RGPD.
[147] CNIL, « Position sur les conditions de déploiement de caméras… », *op. cit*., p. 13.
[148] Art. 25 RGPD.
[149] CNIL, « Position sur les conditions de déploiement de caméras… », *op. cit*., p. 13.

à éviter tout piratage des données enregistrées par le logiciel, ce qui représenterait un risque considérable pour les personnes concernées et leur droit à la vie privée.

Il s'agira, à titre d'exemple, de mettre en œuvre « certaines garanties concernant la qualité des images (abaissement de la définition, floutage, etc.), le nombre d'images traitées, le traitement local des données, l'intégration de mécanismes permettant la suppression quasi immédiate des images sources ou la production d'informations anonymes »[150].

Enfin, la CNIL nous donne un canevas clair, nous permettant d'évaluer la proportionnalité ou non d'un dispositif de vidéosurveillance intelligente. Selon elle, « le caractère proportionné du recours à des dispositifs de vidéo « augmentée » au regard de la finalité recherchée pourra être évalué au regard :

- des **caractéristiques du dispositif** envisagé et de la possibilité - ou de l'impossibilité - de mettre en œuvre de dispositifs moins intrusifs (en termes de nature des données collectées, d'impact sur l'exercice des droits des personnes, d'accoutumance pour les personnes concernées etc.) ;

- des **traitements de données impliqués** (volume des données traitées et éventuelle présence de données sensibles ou de données relatives à des personnes vulnérables, etc.);

- des **conditions de mise en œuvre** (périmètre de déploiement du dispositif dans l'espace et dans le temps et notamment nombre de caméras concernées, durée du déploiement, etc.) ;

- des **garanties** pour limiter l'impact sur les droits et libertés des personnes concernées (anonymisation, minimisation des données, durée de conservation limitée, etc.) »[151].

Or, c'est précisément sur ces points que les réfractaires de la VSA s'insurgent. Selon eux, l'instauration d'une telle technologie dans l'espace public n'est pas nécessaire, et encore moins proportionnelle. La menace pour nos droits fondamentaux ne serait dès lors pas justifiée en droit.

Concernant le projet français, des organisations de la société civile estiment que « ce projet de loi présente des risques élevés pour les droits fondamentaux. Et malgré les preuves existantes de l'inefficacité de la vidéosurveillance en matière de prévention des infractions et des menaces à la sécurité, le gouvernement n'a pas démontré la conformité de ce projet de loi aux principes de nécessité et de proportionnalité et il n'a pas engagé de véritable dialogue avec la société civile au sujet de cette mesure »[152].

Dès lors, elles estiment que « les restrictions des droits humains introduites ne satisfont pas aux trois critères de **légalité**, de **but légitime** et de **nécessité** et de **proportionnalité** »[153].

C'est également l'avis de Katia ROUX, spécialiste Technologies et Droits humains de l'ONG, qui affirme qu' « au regard du droit international, la législation doit répondre

[150] *Ibidem.*
[151] *Ibidem.*
[152] AMNESTY INTERNATIONAL *et al.*, *op. cit.,* p. 3.
[153] *Ibidem.*

strictement à des critères de nécessité de proportionnalité. Or là, le législateur n'en a pas fait la démonstration. On parle d'une technologie d'évaluation, qui doit évaluer les comportements et les catégoriser comme à risque dans le but de prendre des mesures par la suite »[154].

Ainsi, selon certains, « en l'état, cette mesure menace l'essence même du droit à la vie privée et à la protection des données, ce qui la rend **contraire au droit international et européen relatif aux droits humains** »[155].

En revanche, pour la CNIL et le Parlement français, « les garanties encadrant le dispositif permettraient de satisfaire les exigences de sécurité et de protection des personnes concernées, à savoir :

- Le **respect du cadre juridique applicable** (RGPD et loi *Informatique et Libertés*) ;

- **L'exclusion du traitement des données biométriques** ;

- Un **espace temporel et géographique limité**, le dispositif prenant place dans un périmètre géographique limité et ce, jusqu'au 31 mars 2025;

- Une **finalité déterminée et licite**: un décret, pris après avis de la CNIL, fixera les caractéristiques essentielles de ce traitement, en indiquant notamment les événements prédéterminés qu'il aura pour objet de signaler, les spécificités des situations justifiant son emploi, les conditions d'habilitation des agents pouvant accéder à ses résultats ;

- Un **contrôle de la proportionnalité et de l'apport du dispositif**, grâce à une analyse d'impact relative à la protection des données et à une analyse des risques éventuels créés par le dispositif ;

- La **préservation de l'autonomie de la décision humaine et de contrôle humain** : les traitements permettront seulement d'émettre un signal d'attention, limité à l'indication du ou des événements qu'ils auront été programmés à détecter. Un mécanisme de gestion des risques permet de prévenir et de corriger la survenue de biais éventuels ou de mauvaise utilisation ;

- La **loyauté et la pertinence des données** d'apprentissage, de validation et de test ;

- La **supervision et la traçabilité** du dispositif, qui feront l'objet d'un rapport. La CNIL hérite également d'un rôle de contrôle et d'accompagnement dans toutes les phases successives de l'expérimentation »[156].

Néanmoins, lorsqu'il s'agit de reconnaissance faciale, la CNIL avait déjà fait part de ses réserves à propos de l'expérimentation d'un « portique virtuel » de contrôle d'accès par reconnaissance faciale à l'entrée de deux lycées de la région (lycée les Eucalyptus à Nice et lycée Ampère à Marseille). Ce dispositif « devait permettre d'assister les agents en charge du

[154] R. HOUEIX, *op. cit.*
[155] AMNESTY INTERNATIONAL *et al.*, *op. cit.,* p. 2.
[156] J. MAZILLIER, *op. cit.*, p. 177.

contrôle d'accès aux lycées afin de prévenir les intrusions et les usurpations d'identité et de réduire la durée de ces contrôles »[157].

La CNIL avait alors considéré que le dispositif était contraire aux principes de proportionnalité et de minimisation des données posés par le RGPD, dans la mesure où « les objectifs de sécurisation et la fluidification des entrées dans ces lycées peuvent être atteints par des moyens bien moins intrusifs en termes de vie privée et de libertés individuelles, comme par exemple un contrôle par badge »[158].

Cet exemple nous montre dès lors qu'une analyse au cas par cas est pour l'instant la seule envisagée en Europe, à défaut d'un cadre légal clair pour tous. Nous nous retrouvons ainsi face à des décisions divergentes de la CNIL, qui doit se pencher sur les critères de proportionnalité et de nécessité pour chaque utilisation des technologies dans l'espace public.

Il n'est donc pas aisé de déterminer à l'avance si un dispositif tel que la VSA sera ou non considéré comme répondant à de telles exigences, permettant ainsi une ingérence justifiée dans nos droits.

Nous voyons dès lors la fine frontière qui existe entre l'objectif de sécurité et la sauvegarde de nos libertés fondamentales. Il s'agit de trouver le juste **équilibre** à respecter, le tout encadré juridiquement et justifié par la nécessité et la proportionnalité du dispositif mis en place.

De fait, l'un ne doit pas primer sur l'autre: la sauvegarde de nos droits ne devrait pas être un frein à notre sécurité, tout comme l'objectif de protection de la population ne devrait pas annihiler nos libertés.

Une balance que le projet français tente a priori de mettre en place au travers de garanties. Il restera à voir si, en pratique, celles-ci seront effectivement mises en place.

En outre, l'arrivée de l'AI Act devrait nous éclaircir sur la légalité ou non de telles technologies, et sur la véritable définition de la VSA. Si le projet de loi exclut le traitement de données biométriques, l'analyse de comportements est quant à elle considérée comme tel dans le projet de règlement européen. Une interprétation qui sera laissée aux mains des députés européens, et qui nous confirmera ou non la conformité du dispositif français au droit de l'Union.

SECTION 2. RISQUES LIÉS À L'UTILISATION DE LA VIDÉOSURVEILLANCE ALGORITHMIQUE

Si la VSA représente une menace pour nos libertés fondamentales, d'autres risques peuvent également découler de l'utilisation de ce type de technologies au sein de l'espace public. Dans le cadre de la présente section, nous nous pencherons sur trois problématiques créées par les caméras « intelligentes » : le risque de discrimination (*§1*), le glissement vers une surveillance de masse (*§2*) et les dérives d'utilisation de la VSA déjà présentes chez nos voisins (*§3*).

[157] CNIL, « Expérimentation de la reconnaissance faciale dans deux lycées : la CNIL précise sa position », disponible sur www.cnil.fr, 29 octobre 2019.
[158] *Ibidem.*

§1. Biais algorithmique : la porte ouverte aux discriminations ?

Nous l'avons vu, la VSA a ceci de particulier qu'il s'agit de la vidéosurveillance telle que nous la connaissons, mais à laquelle vient se rajouter une couche d'algorithme. Cet algorithme est précisément ce qui peut venir créer des risques de discrimination au sein de la population, violant ainsi les articles 10 et 11 de notre Constitution.

Mais *pourquoi l'algorithme serait-il à l'origine de situations discriminatoires ?* Pour le comprendre, il nous faut remonter jusqu'à la conception du logiciel de VSA. Au moment de la création de l'algorithme, le concepteur se devra de faire des choix, parfois politiques. De fait, lorsque la VSA est utilisée en vue d'un objectif de sécurité, l'être humain à la tête de l'algorithme devra se poser la question suivante : *qu'est-ce qu'un comportement « suspect » ou « anormal » ?*

Le danger est qu'en répondant à cette question au travers de son propre regard, « les algorithmes soient entraînés à travers un jeu de données décidées et conçues par l'être humain. Ils pourront donc intégrer tout simplement les biais discriminatoires de la personne qui les a conçus et pensés »[159].

A cet égard, l'avocat Arnaud TOUATI souligne que « la VSA a déjà été utilisée à des fins racistes, notamment par la Chine, dans la surveillance exclusive des Ouïghours, minorité musulmane présente dans le pays ». Il rappelle également, et à juste titre, que « du fait de la sous-représentation des minorités ethniques dans les données fournies aux algorithmes pour leur apprentissage, il existe des biais discriminatoires et racistes non négligeables »[160].

Ainsi, nous nous apercevons qu'un algorithme peut être victime des biais discriminatoires des concepteurs eux-mêmes, mais également de ceux présents dans les données utilisées pour leur apprentissage. Dans ce second cas, il s'agit de biais qui ne sont pas détectables *a priori* au moment de la conception. Les biais ne seront malheureusement révélés qu'après utilisation de l'algorithme, comme ce fut par exemple le cas de COMPAS, un logiciel de prédiction de récidive de criminels avec des biais racistes envers les personnes afro-américaines[161].

Revenons à présent à la question primordiale à laquelle il convient de répondre : *qu'est-ce qu'un comportement « suspect » ou « anormal » ?*

Selon la Quadrature du Net, « les logiciels de VSA imitent le comportement des agents de police des CSU. Un comportement suspect est donc tout comportement qu'un agent de police qualifierait comme tel, sans qu'il soit nécessairement la base d'une infraction. En pratique, il s'agit de détecter des choses très banales : des objets abandonnées, des personnes qui courent, des regroupements de personnes, des personnes statiques,… En bref, tous les usages de l'espace public qui s'éloignent du seul usage légitime qu'on puisse faire de la rue d'un point de vue policier : se déplacer d'un point à un autre »[162].

Dès lors, l'association établit le constat suivant : plus nous passons de temps dans la rue, plus nous serions suspect du point de vue de la VSA. Ainsi, elle souligne que « les premières

[159] R. HOUEIX, *op. cit.*
[160] *Ibidem*.
[161] A. LOUVIGNY, « Etats-Unis: un logiciel de prédiction des récidives aux penchants racistes », disponible sur www.rtbf.be, 24 mai 2016.
[162] LA QUADRATURE DU NET, « Les dangers de… », *op. cit.*

personnes victimes de cette technologie sont donc les personnes qui vivent ou travaillent dans la rue, parce qu'elles n'ont pas de domicile ou parce qu'elles ont moins accès à des espaces privés. Cette technologie de normalisation des espaces publics s'en prend donc particulièrement aux populations les plus précaires et les plus marginalisées »[163].

De fait, nous pensons également aux personnes qui seraient porteuses d'un handicap. A titre d'exemple, une personne autiste pourrait avoir un comportement considéré comme « suspect », selon l'algorithme : les expressions du visage, la position statique ou encore l'anxiété ressentie dans la foule pourrait provoquer chez la personne autiste des comportements jugés comme étant « anormaux » par une IA.

Par conséquent, il est légitime de se demander si ce genre de choses *peuvent réellement être codifiées sans créer inéluctablement un risque de discrimination.*

L'opacité de l'algorithme, les choix politiques que représente la conception de celui-ci et la difficulté de savoir réellement ce qui constitue un « comportement suspect », nous font penser qu'une codification de ces éléments reste compliquée et se doit, en tout état de cause, d'être extrêmement régulée et contrôlée.

Malgré cela, « ces questions, pourtant politiques, ne sont jamais collectivement discutées, ce qui n'empêcherait donc pas qu'à l'avenir, d'autres situations ou comportements puissent devenir suspects »[164]. Concernant le projet français, le député Modem, Philippe LATOMBE, tente de rassurer la population en affirmant que des garde-fous ont été mis en place, afin de s'assurer que « les appels d'offres soient uniquement réservés à des entreprises qui respectent un certain nombre de règles, dont l'hébergement des données sur le territoire national, le respect de la CNIL et du RGPD »[165]. L'avenir seul nous dira si ces garanties seront suffisantes pour éviter les risques que nous venons d'évoquer.

§2. <u>Le glissement vers la surveillance de masse : l'idée du panoptique</u>

Nous le savons, la VSA peut créer chez certains le sentiment que notre société bascule vers une surveillance de masse.

Et pour cause, Emmanuelle DE CHAMPS, Professeure de civilisation britannique, s'intéresse fortement à ce phénomène de surveillance au sein de notre société. Elle souligne qu'à notre époque, compte tenu de l'évolution de la technologie, nous disposons de tous les moyens nécessaires pour mettre en place une surveillance et une traçabilité permanente des individus, que ce soit dans leur vie privée ou leur vie publique, de par l'usage de leur carte bancaire, de leur téléphone mobile, d'Internet ou encore des caméras présentes dans la rue[166]. Selon la Professeure, l'un des problèmes majeurs de notre société est le contrôle des données, à savoir *qui* peut accéder à ces données.

Mais l'idée du « voir sans être vu » n'est pas survenue au XXIème siècle. De fait, c'est en 1791 que le philosophe Jeremy BENTHAM invente une prison appelée le *panoptique*. Sans le savoir, il crée l'ancêtre de la société de surveillance.

---

[163] *Ibidem.*
[164] *Ibidem.*
[165] R. HOUEIX, *op. cit.*
[166] FRANCE CULTURE, « À l'origine de la société de surveillance : le panoptique », disponible sur www.youtube.com, 3 décembre 2019.

Le panoptique est un dispositif destiné aux prisons britanniques. Le projet consiste à créer un bâtiment rond, avec en son centre une tour de surveillance. Le gardien peut observer les prisonniers sans être vu. L'idée de Bentham n'est pas seulement de surveiller les prisonniers, mais surtout de permettre la réforme morale de l'individu, en leur ôtant l'idée de faire du mal parce qu'ils se savent surveillés. Selon lui, son modèle est adaptable aux écoles, aux hôpitaux et à la politique[167].

En 1975, Michel FOUCAULT, un philosophe français, publie « surveiller et punir ». Dans son œuvre, il s'intéresse à l'idée selon laquelle « le surveillé, pensant être observé, intègre la norme de bonne conduite. Le contrôle social serait ainsi incorporé par les individus »[168].

Le problème de ce genre de dispositif reste l'aspect non-démocratique de celui-ci : « Qui garde les gardiens ? Qui surveille les surveillants ? ». Bentham y avait réfléchi en permettant au public d'accéder à la prison au travers de couloirs, afin de surveiller non seulement les prisonniers, mais également la façon dont ils étaient traités par les surveillants[169].

Ainsi, nous observons qu' « au fil des ans, le panoptique n'a pas disparu mais s'est transformé. Voir sans être vu, nous rappelle les révélations d'Edward Snowden en 2016[170] : l'idée du panoptique s'est aujourd'hui numérisée. Et si les médias font souvent référence au « Big Brother », nous basculons plutôt aujourd'hui vers une « Big Mother », qui épie tout en « rendant service ». Nous serions observés pour notre bien - par exemple, pour notre sécurité. Il s'agit donc d'une « tour de contrôle beaucoup mieux dissimulée » [171].

Cette surveillance constante est devenue notre norme. A cet égard, l'ONU dénonçait l'année dernière une augmentation de la surveillance dans les espaces publics de certains pays, notamment à cause de la reconnaissance biométrique, en vue de surveiller les opposants politiques ou procéder à du profilage racial[172].

La VSA, de par sa nature, constitue « un passage à une autre échelle, qui change la nature de la surveillance »[173]. L'idée de « safe city » et de « smart city » se développent de plus en plus, notamment en France dans plus de 200 villes[174], parmi lesquelles nous retrouvons Nice, Marseille, Saint-Etienne ou encore Valenciennes[175].

La CNIL met également en garde sur « les risques importants pour les libertés individuelles ou collectives qui existent du simple fait de la multiplication des dispositifs de vidéo « augmentée » qui pourrait aboutir à un sentiment de surveillance généralisée »[176].

---

[167] *Ibidem.*
[168] *Ibidem.*
[169] *Ibidem.*
[170] Cour eur. D.H. (gde ch.), arrêt *Big Brother Watch et autres c. Royaume-Uni*, 25 mai 2021.
[171] *Ibidem.*
[172] M-L. MATHOT, « Les gens sont de plus en plus surveillés dans les espaces publics, notamment à cause de la reconnaissance biométrique, dénonce l'ONU », disponible sur www.rtbf.be, 16 septembre 2022.
[173] E. LECLÈRE, « La vidéo-surveillance algorithmique, « un passage à une autre échelle, qui change la nature de la surveillance » », disponible sur www.radiofrance.fr, 23 janvier 2023.
[174] LA QUADRATURE DU NET, « Stratégies d'infiltration de la surveillance biométrique dans nos villes et nos vies », disponible sur www.laquadrature.net, 23 février 2023.
[175] M. PICAUD, « Peur sur la ville. La sécurité numérique pour l'espace urbain en France », Rapport de recherche 01/2021, Chaire « Villes et numérique », *Ecole urbaine de Sciences Po*, 2021.
[176] CNIL, « Position sur les conditions de déploiement de caméras… », *op. cit*., p. 9.

Ainsi, le projet concernant les JO 2024 soulève de nombreuses questions en la matière, certains estimant de surcroît qu'il s'agira bel et bien de surveillance biométrique[177].

De fait, selon des organisations de la société civile, « si l'usage de caméras dotées d'algorithmes est destiné à détecter des évènements suspects spécifiques dans l'espace public, ces caméras capteront et analyseront forcément des traits physiologiques et des comportements de personnes présentes dans ces espaces. Il pourra s'agir de la posture de leurs corps, de leur démarche, de leurs mouvements, de leurs gestes ou de leur apparence. Le fait d'isoler des personnes par rapport à leur environnement, qui s'avère indispensable en vue de remplir l'objectif du système, constitue une « identification unique ». Tel que l'établit la loi sur la protection des données de l'UE et selon l'interprétation du Comité européen de la protection des données[178], la capacité d'isoler une personne parmi une foule ou par rapport à son environnement, que son nom ou son identité soient connus ou non, constitue une « identification unique »[179].

Si tel est le cas, le sentiment de surveillance n'en serait que renforcé. Nous serions face à un cas où nos libertés seraient mises à mal pour le *fantasme d'une police prédictive*, qui s'inscrit dans la lignée de la « Big Mother » que nous évoquions.

Il reste toutefois à établir un équilibre juridique et éthique, pour éviter tout débordement vers une surveillance démesurée, créant un sentiment de paranoïa au sein de la population, pouvant mener, comme nous le soulignons, vers une autolimitation de nos libertés.

§3. Illustrations de dérives potentielles

Jusqu'ici, certains lecteurs se posent peut-être la question suivante : si je n'ai rien à cacher, pourquoi est-ce si important de protéger mon droit à la vie privée ?

A cet égard, Edward SNOWDEN a déclaré : « *Dire que votre droit à la vie privée importe peu car vous n'avez rien à cacher revient à dire que votre liberté d'expression importe peu car vous n'avez rien à dire. Car même si vous n'utilisez pas vos droits aujourd'hui, d'autres en ont besoin. Cela revient à dire: les autres ne m'intéressent pas* ».

Par conséquent, deux constats peuvent être établis. Sur un plan individuel, chacun a au moins une chose à cacher : son intimité. Sur le plan collectif, si nous n'avons rien à cacher dans un domaine, il se peut que pour d'autres ce ne soit pas le cas. Certaines personnes pourraient ne pas vouloir que certaines données sortent de la sphère privée (*par exemple: être atteint de maladie mentale*)[180].

Ainsi, si le droit à la vie privée se doit d'être protégé, les dérives d'utilisation de technologies telles que la VSA sont à éviter. Et ces dérives ne sont pas à prendre à la légère. Il ne s'agit pas d'hypothèses qui pourraient arriver mais de situations déjà existantes dans d'autres pays.

---

[177] AMNESTY INTERNATIONAL *et al.*, *op. cit*.
[178] EDPB, *op. cit.*
[179] AMNESTY INTERNATIONAL *et al.*, *op. cit*.
[180] C. DE TERWANGNE, Cours magistral du Master DTIC UNamur de « Vie privée et protection des données », *Chapitre I. TIC et nouveaux défis pour la vie privée*, slide 30, 15 septembre 2022.

En Chine, le gouvernement a mis en place le crédit social, afin de palier la difficulté chronique dans l'application des lois et des règlements[181]. Lorsqu'il s'agit de présenter le système de crédit social chinois, « il est souvent fait allusion à la série télévisée *Black Mirror* dont l'un des épisodes donne à voir une société dans laquelle les individus s'évaluent en permanence en s'attribuant des notes au gré des interactions qu'ils ont avec les uns ou avec les autres »[182].

L'objectif du crédit social chinois est de classer les citoyens, en se basant sur plusieurs critères. Il s'agira d'évaluer les comportements de chaque individu, dans les espaces publics ou encore sur internet, pour lui accorder ou non des récompenses et des sanctions. Ce classement est rendu possible grâce aux nombreuses données que possèdent le gouvernement chinois, qui sont ensuite soumises à une intelligence artificielle « afin qu'elle les étudie et attribue des « points» aux individus »[183]. A titre d'exemple, nous retrouvons parmi ces données des informations bancaires (revenus, achats, factures impayées), institutionnelles (parcours scolaires, situation familiale) ou encore étatiques[184].

« En plus de ces données factuelles, les actions des citoyens sont également évaluées dans la notation du crédit social. Ainsi, un individu qui œuvre pour la communauté, respecte le Code de la route et se montre serviable avec les autres verra sa note augmenter. En revanche, ceux qui ont des dettes, transgressent les règles du Code de la route ou laissent traîner leur poubelle devant chez eux perdront des points.

Pour pouvoir surveiller et noter le comportement de ses citoyens en société, le gouvernement chinois se repose sur son immense système de caméras de surveillance. Le pays compte plus de 200 millions de vidéosurveillances, dont une bonne partie est équipée d'un système de reconnaissance faciale.

Une technologie essentielle pour repérer et identifier les auteurs d'incivilités et d'infractions dans les villes. En permanence, les caméras épient les moindres faits et gestes de la population chinoise. Lorsqu'une caméra repère un comportement douteux – par exemple, un automobiliste ivre -, elle identifie son auteur et indique au système de notation que celui-ci a commis une infraction. Le « mauvais » citoyen perdra alors des points de crédit social »[185]. Dès lors, nous constatons que la Chine prône une « contrôlocratie »[186], rendue possible notamment grâce à l'intelligence artificielle.

En Iran, ce sont les droits de femmes qui pourraient être mis à mal puisque la reconnaissance faciale pourrait cette fois servir à verbaliser les femmes qui ne portent pas de hijab. En effet, en septembre 2022, « des médias iraniens ont révélé que les autorités envisageaient d'appliquer la reconnaissance faciale aux images de vidéosurveillance, pour sanctionner les femmes dont la tenue est jugée impudique »[187].

---

[181] S. ARSÈNE, « Le système de crédit social en Chine. La discipline et la morale », *Réseaux*, n°225, 2021/1, p. 55 à 86.
[182] B. LE GALL, « Système de crédit social chinois : outil de contrôle social ou modèle de société pérenne ? », *Revue Défense Nationale*, n°828, 2020/3, p. 101 à 106.
[183] J. MERTENS, « Comment fonctionne le « crédit social » en Chine », disponible sur www.geeko.lesoir.be, 27 juillet 2019.
[184] *Ibidem.*
[185] J. MERTENS, *op. cit.*
[186] L. MONTALTE, « Contrôlocratie : l'enfer est pavé de pseudo-bonnes intentions », disponible sur www.questionchine.net, 1er septembre 2020.
[187] P. SUGY, « En Iran, la reconnaissance faciale pourrait servir à verbaliser les femmes qui n'ont pas de hijab », disponible sur www.lefigaro.fr, 20 septembre 2022.

En Israël, un contrôle sur la population palestinienne est effectué via un système expérimental de reconnaissance faciale appelé *Red Wolf*[188]. Cette technologie provoque ainsi un renforcement de l'apartheid, puisqu'elle vise à « pister les Palestiniens et les Palestiniennes, et automatiser les très strictes restrictions de leur droit de circuler librement »[189].

Nous voyons donc au travers de ces exemples, que les dérives nous entourent et constituent, malheureusement, une réalité dans le monde actuel.

Ainsi, si les avancées technologiques peuvent être bénéfiques pour notre société, le tout est de ne pas sombrer dans l'extrême utilisation de tels dispositifs dans l'espace public.

Par conséquent, une réglementation claire et stricte nous paraît primordiale afin d'éviter les risques que peuvent poser la VSA. Un équilibre se doit d'être maintenu : l'Europe ne peut se permettre de basculer vers une société de surveillance, où nos droits fondamentaux seraient annihilés sans justification de proportionnalité ni de nécessité.

Une approche que le Parlement européen tente d'ailleurs de suivre actuellement en élaborant le premier texte au monde régulant l'intelligence artificielle.

SECTION 3. PISTES DE SOLUTIONS

Nous l'avons vu, si la VSA peut présenter des avantages, elle peut également être à l'origine de dérives, créant un environnement défavorable pour l'exercice de nos droits. Dès lors, une question se pose : *un équilibre peut-il être trouvé entre efficacité technologique et sauvegarde de nos libertés fondamentales ?* Une réflexion qui mène à deux postulats possibles.

Le premier – et le plus extrême – est celui adopté par de nombreuses associations protectrices de droits fondamentaux[190] : un tel équilibre ne peut être trouvé, si bien que seule **l'interdiction** de la VSA est envisageable. Elles estiment en effet que l'utilisation de la reconnaissance faciale, qui est une application de la VSA, au sein de l'espace public présente trop de risques pour notre société.

Or, une évolution technologique paraît pourtant inévitable… Une remarque à laquelle Noémie LEVAIN, juriste à la Quadrature du Net, répond en faisant référence au fait qu'au cours de l'Histoire, certaines découvertes scientifiques, jugées trop dangereuses, n'ont pas connu de suite favorable[191]. Tel fut le cas du clonage, par exemple, qui est en principe interdit[192] – sauf pour usage thérapeutique[193].

Ainsi, lorsque la technologie va trop loin, il faudrait apprendre à rebrousser chemin, selon les défenseurs de droits fondamentaux. Une philosophie avec laquelle la ville de Lausanne est en

---

[188] AMNESTY INTERNATIONAL, « Comment israël renforce son contrôle sur la population palestinienne via la reconnaissance faciale », disponible sur www.amnesty.fr, 2 mai 2023.
[189] AMNESTY INTERNATIONAL, « Israël, la reconnaissance faciale renforce l'apartheid », disponible sur www.amnesty.be, 2 mai 2023.
[190] EDRI, *op. cit.*; X, « Pour l'interdiction de la reconnaissance faciale à Bruxelles », disponible sur www.democratie.brussels, 6 mars 2023. ; X, « Reclaim your face », disponible sur www.reclaimyourface.eu, *s.d.,* consulté le 20 juin 2023.
[191] FRANCE CULTURE, *op. cit.*
[192] Loi du 11 mai 2003 relative à la recherche sur les embryons in vitro, *M.B.*, 28 mai 2003, art. 6.
[193] Loi du 11 mai 2003 précitée, art. 3, 1°.

parfait accord, puisqu'elle a récemment interdit l'utilisation de systèmes de reconnaissance faciale dans l'espace public[194].

Mais si pour certains la reconnaissance faciale dans l'espace public et d'autres formes de surveillance biométrique de masse portent atteinte à un large éventail de droits fondamentaux, les autorités et les entreprises européennes ne se privent pas de déployer ces systèmes à grande vitesse[195]. C'est ainsi que, par exemple, nous avons pu constater l'installation de la VSA dans certaines villes de France, ou encore l'utilisation de technologies similaires en Belgique par les forces de l'ordre.

Si jusqu'ici ces utilisations étaient illégales car elles ne reposaient sur aucun texte juridique, la situation a aujourd'hui évolué avec la nouvelle loi française concernant le déploiement de la VSA lors des JO 2024. En Belgique, la question du contrôle juridique de la VSA est également intéressante puisque suite à son utilisation illégale, certains députés ont déclaré ne pas être contre l'idée d'instaurer de telles technologies dans l'espace public si celles-ci étaient légalement encadrées.

Par conséquent, si la Quadrature du Net se réfère à l'Histoire, nous pouvons également nous rappeler que, plus d'une fois, l'être humain n'a pas tiré les leçons du passé. Ainsi, le second postulat repose sur le fait qu'à la vue de ces différents éléments, nous pouvons légitimement penser que plutôt que de suivre le chemin de la prudence, les dirigeants européens préconisent le développement de leur **stratégie numérique.**

Malgré tout, comme nous l'avons déjà souligné, la mise en place de tels dispositifs créerait une ingérence telle dans nos droits qu'il est nécessaire que celle-ci repose sur un cadre juridique clair et harmonisé.

L'AI Act serait un premier pas vers l'encadrement de la VSA. Les députés européens ont par ailleurs une approche nuancée, incluant les deux postulats que nous venons d'évoquer. De fait, le texte prévoit l'interdiction de certains dispositifs, par exemple la reconnaissance faciale, ce qui éviterait des dérives telles que le crédit social chinois. Mais en optant pour une approche par les risques, des développements techniques sont tout de même possible en matière d'IA. Il suffira dès lors de respecter un certain nombre d'exigences, notamment d'assurer une plus grande transparence des dispositifs.

A ce stade, l'AI Act n'étant pas encore entré en vigueur, il ne nous est pas possible d'affirmer qu'un tel encadrement est suffisant pour éviter les risques inhérents à la VSA. Toutefois, certains estiment déjà que la loi proposée n'impose pas une interdiction de la plupart des cas de surveillance biométrique de masse, ce qui ne règlerait donc pas la menace que la surveillance biométrique de masse fait peser sur nos libertés[196]. Néanmoins, il faudra laisser le temps au temps, afin de constater si oui ou non, la nouvelle législation européenne tend véritablement à sauvegarder nos droits et à contrôler de manière efficiente l'utilisation de la VSA au sein de l'espace public.

---

[194] VAUD, « Lausanne interdira la reconnaissance faciale dans l'espace public », disponible sur www.rts.ch, 29 mars 2023.
[195] Traduction libre de EDRI, « Facial Recognition & Biometric Mass Surveillance: Document Pool », disponible sur www.edri.org, 25 mars 2020.
[196] Traduction libre de EDRI, « New AI law proposal calls out harms of biometric mass surveillance, but does not resolve them », disponible sur www.edri.org, 22 avril 2021.

Conclusion

C'est alors que nous arrivons au bout de notre analyse. Au terme de notre travail, nous avons pu nous intéresser à ce que recouvre la vidéosurveillance algorithmique et avons pu constater qu'une définition d'un tel dispositif n'est pas chose aisée.

S'agit-il de surveillance biométrique ou non ? Une question à laquelle une réponse ne peut pour l'instant être apportée, même si, selon nous, il n'est pas exclu que l'interprétation du Comité européen de la protection des données, qui estime que « la capacité d'isoler une personne parmi une foule ou par rapport à son environnement, que son nom ou son identité soient connus ou non, constitue une « identification unique »[197], soit retenue par les eurodéputés lors de l'élaboration de l'AI Act.

Cette controverse explique en partie pourquoi il est si difficile de lui trouver un cadre juridique applicable. Ne sachant pas réellement dans quelle catégorie ranger la VSA, il est compliqué de savoir quels textes mobiliser.

C'est pourquoi, en premier lieu, nous nous sommes penchés sur le cadre existant, mais également à venir, en Europe. Si le RGPD protège le traitement de nos données à caractère personnel et par voie de conséquence notre droit à la vie privée, l'intelligence artificielle quant à elle ne fait pas encore l'objet d'un encadrement.

La Commission européenne tente néanmoins d'y remédier en proposant l'AI Act, qui serait la première loi régissant l'IA au monde. La question de la définition de la VSA pourrait dès lors être résolue par les députés européens, même si nous nous apercevons, au travers du projet français pour les JO 2024, qu'il est aisé de passer entre les mailles du filet. Toutefois, le fait de réguler l'IA reste une bonne chose. Des ajustements devront simplement, comme pour toute législation, être faits suivant les failles observées lors de l'application pratique du texte.

De plus, les exemples d'utilisations de VSA en Europe nous ont montré que malgré un cadre légal – comme c'est le cas en France – les garanties ne suffisent parfois pas à éviter certains risques. En outre, le cas de la Belgique nous a également démontré que de telles technologies sont parfois utilisées même sans encadrement juridique. Dès lors, nous pouvons craindre que le déploiement de la VSA en Europe encouragerait ce type de comportements, chaque État membre voulant également suivre le mouvement de l'innovation technologique. Il est à espérer que l'AI Act viendra harmoniser la matière et que chaque pays membre de l'Union suivra les règles qu'il instaure en matière d'intelligence artificielle.

En second lieu, nous avons analysé les différents risques liés au déploiement de la VSA au sein de l'espace public.

Nous avons alors pu constater le danger que cela représente pour nos libertés fondamentales, notamment avec le risque d'autolimitation. Celui-ci est évidemment lié au sentiment de surveillance généralisée qu'instaure l'utilisation de ce genre de dispositifs dans la sphère publique. Il s'agit là de l'idée du panoptique : voir sans être vu.

Si certes, le droit à la vie privée n'est pas absolu, il n'en demeure pas moins que pour créer une telle ingérence dans nos droits, les mesures de sécurité prises par les forces de l'ordre se doivent

[197] AMNESTY INTERNATIONAL *et al.*, *op. cit.*

d'être nécessaires et proportionnées. Or, comme l'ont souligné certains réfractaires au projet français, ce dernier ne répond pas à de telles exigences, notamment du fait qu'une réelle efficacité de la VSA n'a jamais pu être prouvée.

Il est alors tentant de penser que le gouvernement français, à cet égard, bascule sans doute vers un *solutionnisme technologique*. Selon nous, le danger de la VSA réside dans le fait de ne pas justifier en droit son utilisation. La proportionnalité et la nécessité doivent impérativement être respectées pour qu'il y ait ingérence dans nos droits.

C'est également l'avis de Katia ROUX, spécialiste Technologies et Droits humains de l'ONG, qui estime que « cette technologie est, en soi, problématique et dangereuse pour les droits humains et qu'elle le restera tant qu'il n'y aura pas eu une sérieuse évaluation, tant qu'il n'y aura pas eu de démonstration de la nécessité et de la proportionnalité de son usage, et tant qu'il n'y aura pas eu de véritable débat avec les différents acteurs de la société civile sur la question »[198].

Ainsi, sans justification de la part du gouvernement, nous basculerions vers un sacrifice de nos libertés fondamentales au profit du fantasme d'une police prédictive, dont l'efficacité n'a jusqu'à aujourd'hui pas pu être démontrée…

Enfin, il convient de ne pas oublier que des dérives plus graves encore existent et constituent une réalité dans la société actuelle. C'est le cas du crédit social chinois, ou encore de la situation israélienne ou iranienne. Par conséquent, la question de la transparence de l'utilisation de la VSA mais également de l'algorithme utilisé par le logiciel, nous paraît être cruciale lorsque des droits humains sont en jeu. Dès lors, nous estimons qu'un contrôle démocratique des algorithmes utilisés dans le secteur public est nécessaire, même si sa mise en pratique paraît complexe au vu de l'opacité de ces derniers.

Pour finir, s'agissant des pistes de solutions envisagées, nous ne sommes pas pour une interdiction de l'utilisation de technologies dans l'espace public. Nous sommes plutôt en faveur d'un cadre clair et harmonisé au sein de l'Union européenne, afin que chaque État membre s'aligne sur le sujet. Une harmonisation nous parait primordiale au vu de l'importance des droits en jeu. Selon nous, il convient donc d'établir un accord sur trois points : la protection de la vie privée (RGPD), la réglementation de l'intelligence artificielle (AI Act) et la transparence des algorithmes dans le secteur public.

Pour conclure, il est encore difficile à l'heure actuelle de savoir si l'AI Act sera efficace ou non. Aussi, aucune critique n'a été émise sur la proposition de la Commission en ce qu'il s'agit de la première loi au monde réglementant l'IA : aucune comparaison avec un autre texte légal – européen ou non – ne peut donc être établie. En outre, le texte n'étant pas encore totalement abouti ni appliqué, il est difficile de prédire son efficacité ou non. Par conséquent, si nous avons pu répondre à un certain nombre de questions que nous nous posions, d'autres restent néanmoins en suspens… L'avenir seul nous dira si la stratégie numérique de l'Union européenne aura pu se poursuivre dans le respect de nos droits.

Et comme le disait le célèbre philosophe Sénèque, « en tout, l'excès est un vice ». Ainsi, retenons que tout est une question d'équilibre entre objectif de sécurité et sauvegarde de nos libertés.

[198] R. HOUEIX, *op. cit.*

Bibliographie

I. DROIT INTERNATIONAL ET DROIT EUROPÉEN

1.1. Droit primaire européen

Convention de sauvegarde des droits de l'homme et des libertés fondamentales, signée à Rome le 4 novembre 1950, approuvée par la loi du 13 mai 1955, *M.B.*, 19 août 1955, *err.*, 29 juin 1961.

1.2. Droit dérivé européen

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 119/1, 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.,* L 119/89, 4 mai 2016.

1.3. Travaux préparatoires (des institutions de l'Union européenne)

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.

II. DROIT INTERNE FRANÇAIS

2.1. Législation

Constitution, *JO*, 5 octobre 1958.

Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, *JORF*, 7 janvier 1978.

Loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité, NOR: INTX9400063L, *JORF* n°0020, 24 janvier 1995.

Loi du 24 janvier 2022 relative à la responsabilité pénale et à la sécurité intérieure, NOR: JUSX2116059L, *JORF*, 25 janvier 2022.

Loi n° 2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions, NOR : SPOX2233026L, *JORF* n°0116, 20 mai 2023.

2.2. Travaux préparatoires

Projet de loi adopté par le Sénat, relatif aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions, art. 7, *Assemblée Nationale*, seizième législature, 1er février 2023, n°809.

III. DROIT INTERNE BELGE

3.1. Législation

Constitution coordonnée, *M.B*., 17 février 1994.

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

Loi du 11 mai 2003 relative à la recherche sur les embryons in vitro, *M.B.*, 28 mai 2003.

Loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance, *M.B.*, 31 mai 2007.

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

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

3.2. Travaux préparatoires

Proposition de loi modifiant la loi relative à la publicité de l'administration du 11 avril 1994 afin d'introduire une plus grande transparence dans l'usage des algorithmes par l'administration, *Doc.*, Ch., 55, 2020-2021, n°1904/001.

Proposition de résolution relative à la mise en place d'une autorité de contrôle des algorithmes, *Ann. Parl*., Sén., 2022-2023, séance du 10 février 2023, n°7-328/4.

IV. DOCUMENTS DU CONSEIL D'ÉTAT FRANÇAIS

C.E., Avis du sur un projet de loi relatif aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions, NOR : SPOX2233026L, *Assemblée générale*, n°406383, séance du 15 décembre 2022.

C.E., 17 mai 2023, n° 2023-850 DC.

V. DOCUMENTS DE LA CNIL

CNIL, « Algorithme », disponible sur https://www.cnil.fr, *s.d.,* consulté le 2 mars 2023.

CNIL, « Caméras dites « augmentées » dans les espaces publics : la position de la CNIL », disponible sur www.cnil.fr, 19 juillet 2022.

CNIL, « Déploiement de caméras « augmentées » dans les espaces publics : la CNIL publie sa position », disponible sur www.cnil.fr, 19 juillet 2022.

CNIL, « Expérimentation de la reconnaissance faciale dans deux lycées : la CNIL précise sa position », disponible sur www.cnil.fr, 29 octobre 2019.

CNIL, « Position sur les conditions de déploiement de caméras dites « intelligentes » ou « augmentées » dans les espaces publics », disponible sur www.cnil.fr, juillet 2022.

VI. DOCTRINE

ARSÈNE, S., « Le système de crédit social en Chine. La discipline et la morale », *Réseaux*, n°225, 2021/1, p. 55 à 86.

CASTAGNINO, F., 2019, « Rendre « intelligentes » les caméras : déplacement du travail des opérateurs de vidéosurveillance et redéfinition du soupçon », *Sciences Po*, n°5, 2019.

DEGRAVE, E., MAERTENS C. et ROY, L., « Les droits fondamentaux face aux algorithmes du secteur public », *Dossier Libertés Publiques*, 2023, p. 15 à 17.

LE GALL, B., « Système de crédit social chinois : outil de contrôle social ou modèle de société pérenne ? », *Revue Défense Nationale*, n°828, 2020/3, p. 101 à 106.

MAZILLIER, J., « RGPD : « caméras augmentées » sur le podium olympique : quelles garanties ? », Expertises, n°490, 2023, p. 176 à 177.

PICAUD, M., « Peur sur la ville. La sécurité numérique pour l'espace urbain en France », Rapport de recherche 01/2021, Chaire « Villes et numérique », *Ecole urbaine de Sciences Po*, 2021.

ROZENFELD, S., « Vidéosurveillance algorithmique : le précédent français », *Expertises*, n°489, 2023, p. 112.

VII. JURISPRUDENCE

Cour eur. D.H. (gde ch.), arrêt *Big Brother Watch et autres c. Royaume-Uni*, 25 mai 2021.

VIII. SOURCES INTERNET

ALBERTINI, A., « Une étude commandée par les gendarmes montre la relative inefficacité de la vidéosurveillance », disponible sur www.lemonde.fr, 22 décembre 2021.

ALOUETTE, « Qu'est-ce que la vidéosurveillance algorithmique ? », disponible sur www.technopolice.fr, 29 mars 2022.

AMNESTY INTERNATIONAL, « Comment israël renforce son contrôle sur la population palestinienne via la reconnaissance faciale », disponible sur www.amnesty.fr, 2 mai 2023.

AMNESTY INTERNATIONAL, « Israël, la reconnaissance faciale renforce l'apartheid », disponible sur www.amnesty.be, 2 mai 2023.

COTON, F., « Souriez, vous êtes filmé ! », disponible sur www.lexing.be, 17 mars 2023.

DOSDA, G. et AFP, « Loi sur les JO de 2024 : l'Assemblée adopte un article controversé sur la vidéosurveillance », disponible sur www.lejdd.fr, 23 mars 2023.

EDPB, « Lignes directrices 3/2019 sur le traitement des données à caractère personnel par des dispositifs vidéo », Version 2.0., disponible sur www.edpb.europa.eu, 29 janvier 2020.

FRANCE CULTURE, « À l'origine de la société de surveillance : le panoptique », disponible sur www.youtube.com, 3 décembre 2019.

HOUEIX, R., « Paris-2024 : les JO, cheval de Troie de la vidéosurveillance algorithmique ? », disponible sur www.france24.com, 24 mars 2023.

LA QUADRATURE DU NET, « Les dangers de la vidéosurveillance algorithmique (VSA) », disponible sur www.youtube.com, 15 mars 2023.

LA QUADRATURE DU NET, « Qu'est-ce que la vidéosurveillance algorithmique ? », disponible sur www.laquadrature.net, 23 mars 2022.

LA QUADRATURE DU NET, « Stratégies d'infiltration de la surveillance biométrique dans nos villes et nos vies », disponible sur www.laquadrature.net, 23 février 2023.

LECLÈRE, E., « La vidéo-surveillance algorithmique, « un passage à une autre échelle, qui change la nature de la surveillance » », disponible sur www.radiofrance.fr, 23 janvier 2023.

LE CŒUR, P., « JO 2024 : les députés autorisent la vidéosurveillance algorithmique avant, pendant et après les Jeux », disponible sur www.lemonde.fr, 23 mars 2023, mis à jour le 18 avril 2023.

LELOUP, D., « Adoptée pour les JO de Paris 2024, la surveillance algorithmique n'a jamais fait ses preuves », disponible sur www.lepolitique.net, 10 mars 2023.

L.H. et P.M., « La reconnaissance faciale est en test à Brussels Airport », disponible sur www.rtbf.be, 10 juillet 2019.

LOUVIGNY, A., « Etats-Unis: un logiciel de prédiction des récidives aux penchants racistes », disponible sur www.rtbf.be, 24 mai 2016.

MAQUINDUS, O., « « AI Act » : comment l'UE investit déjà dans des intelligences artificielles à « haut risque » pour contrôler ses frontières », disponible sur www.lemonde.fr, 22 juin 2023.

MATHOT, M-L., « Les gens sont de plus en plus surveillés dans les espaces publics, notamment à cause de la reconnaissance biométrique, dénonce l'ONU », disponible sur www.rtbf.be, 16 septembre 2022.

MERTENS, J., « Comment fonctionne le « crédit social » en Chine », disponible sur www.geeko.lesoir.be, 27 juillet 2019.

MONTALTE, L., « Contrôlocratie : l'enfer est pavé de pseudo-bonnes intentions », disponible sur www.questionchine.net, 1er septembre 2020.

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

REUTERS, AFP et RENSON, L., « Qu'est-ce que l' « AI Act », la législation sur l'intelligence artificielle de la Commission européenne? », disponible sur www.lecho.be, 22 mars 2023.

SUGY, P., « En Iran, la reconnaissance faciale pourrait servir à verbaliser les femmes qui n'ont pas de hijab », disponible sur www.lefigaro.fr, 20 septembre 2022.

VAUD, « Lausanne interdira la reconnaissance faciale dans l'espace public », disponible sur www.rts.ch, 29 mars 2023.

X, « Algorithme : Qu'est-ce que c'est ? A quoi ça sert ? », disponible sur www.datascientest.com, 11 août 2021.

X, « Caméras de surveillance – Nouvelle réglementation ! », disponible sur www.police.be, 12 juillet 2018.

X, « Deep Learning ou Apprentissage Profond : qu'est-ce que c'est ? », disponible sur www.datascientest.com, 28 septembre 2020.

X, « JO 2024 : interdiction de la « reconnaissance faciale et du traitement biométrique », assure Darmanin, la gauche sceptique », disponible sur www.midilibre.fr, 23 mars 2023.

X, « Loi du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions », disponible sur www.vie-publique.fr, 22 mai 2023.

X, « Loi sur l'IA de l'UE : première réglementation de l'intelligence artificielle », disponible sur www.europarl.europa.eu, 9 juin 2023, mis à jour le 14 juin 2023.

X, « Pour l'interdiction de la reconnaissance faciale à Bruxelles », disponible sur www.democratie.brussels, 6 mars 2023.

X, « Pour l'interdiction de la reconnaissance faciale à Bruxelles », disponible sur www.mrax.be, 28 mars 2023.

X, « Sécurité à Paris 2024 : inimaginable « de voir arriver un texte comme ça en France », s'insurgent des députés », disponible sur www.midilibre.fr, 20 mars 2023.

IX. SOURCES ÉTRANGÈRES

EDRI, « Facial Recognition & Biometric Mass Surveillance: Document Pool », disponible sur www.edri.org, 25 mars 2020.

EDRI, « New AI law proposal calls out harms of biometric mass surveillance, but does not resolve them », disponible sur www.edri.org, 22 avril 2021.

EDRI, « Protect My Face: Brussels residents join the fight against biometric mass surveillance », disponible sur https://edri.org, 29 mars 2023.

X, « Reclaim your face », disponible sur www.reclaimyourface.eu, *s.d.,* consulté le 20 juin 2023.

X. DIVERS

ACCESS NOW, INTERNATIONAL, ALGORACE, ESPAGNE, ALGORITHMWATCH, ALLEMAGNE ALGORITHMWATCH CH, SUISSE, AMNESTY INTERNATIONAL, INTERNATIONAL APTI, ROUMANIE, ARTICLE 19, INTERNATIONAL, ASSOCIATION NATIONALE DES SUPPORTERS, FRANCE, BIG BROTHER WATCH, ROYAUME-UNI, BITS OF FREEDOM, PAYS-BAS, CENTRE FOR DEMOCRACY & TECHNOLOGY, EUROPE, CHAOS COMPUTER CLUB LËTZEBUERG, LUXEMBOURG, CITIZEN D / DRŽAVLJAN D, SLOVÉNIE, CIVIL LIBERTIES UNION FOR EUROPE, EUROPE, DEUTSCHE VEREINIGUNG FÜR DATENSCHUTZ E.V. (DVD), ALLEMAGNE DIGITALCOURAGE E.V., ALLEMAGNE, DIGITALE GESELLSCHAFT, SUISSE, DIGITALE FREIHEIT E.V., ALLEMAGNE, ELEKTRONISK FORPOST NORGE, NORVÈGE, ETICAS TECH, ESPAGNE, EUROPEAN CENTER FOR NOT-FOR-PROFIT LAW STICHTING (ECNL), EUROPE EUROPEAN DIGITAL RIGHTS, EUROPE, FAIR TRIALS, INTERNATIONAL, FORUM CIVIQUE EUROPÉEN, FRANCE/EUROPE, FOOTBALL SUPPORTERS EUROPE, EUROPE, HOMO DIGITALIS, GRÈCE, HUMAN RIGHTS WATCH, INTERNATIONAL, IRISH COUNCIL FOR CIVIL LIBERTIES, IRLANDE, IT-POL, DANEMARK, IURIDICUM REMEDIUM, RÉPUBLIQUE TCHÈQUE, LIBERTY, ROYAUME-UNI, PANOPTYKON FOUNDATION, POLOGNE, PRIVACY INTERNATIONAL, INTERNATIONAL, PRIVACY NETWORK, ITALIE, SHARE FOUNDATION, SERBIE, SOCIETY VRIJBIT, PAYS-BAS, STATEWATCH, EUROPE, TODAY IS A NEW DAY / DANES JE NOV DAN, SLOVÉNIE, « Lettre de la société civile aux députés français sur le projet de loi relatif aux Jeux olympiques et paralympiques 2024 », disponible sur www.edri.org, *s.d*., consulté le 15 juin 2023.

Avis de l'Autorité de Protection des Données n° 157/2021 du 10 septembre 2021.

CLUZEL, L., Cours-Conférence donné dans le cadre de la Chaire Francqui en E-gouvernement de l'UNamur, 16 février 2023.

CLUZEL, L., Cours-Conférence donné dans le cadre de la Chaire Francqui en E-gouvernement de l'UNamur, 10 mars 2023.

DE TERWANGNE, C., Cours magistral du Master DTIC UNamur de « Vie privée et protection des données », *Chapitre I. TIC et nouveaux défis pour la vie privée*, slide 30, 15 septembre 2022.