S'opposer à la vidéosurveillance automatisée

11 mars 2022

Depuis trois ans, dans le cadre de sa campagne Technopolice, La Quadrature du Net documente[1] et combat[2] le déploiement en France de dispositifs de « vidéosurveillance automatisée » (VSA) - des caméras visant à détecter automatiquement des comportements surveillés par la police.

Que ce soit la ville de Marseille qui cherche à repérer[3] des comportements « anormaux » avec la SNEF, la ville de Suresnes qui autorise[4] l'entreprise XXII à entraîner ses algorithmes sur sa population ou encore Roubaix qui, comme de très nombreuses villes, a intégré[5] le logiciel Briefcam pour pouvoir faire du suivi de personne, nous observons un développement important de systèmes de vidéosurveillance algorithmique ces dernières années.

L'expérience de notre lutte a permis d'identifier les **raisons politiques** de rejeter cette technologie (partie I) ainsi que les **moyens juridiques** permettant de l'interdire (partie II).

I. Des raisons politiques de s'opposer à la VSA

Les promoteurs de la VSA prétendent chercher un équilibre entre la « sécurité » que produirait cette technologie et les « libertés » auxquelles elle porterait atteinte. Il s'agit d'un faux dilemme. **La VSA va réduire à la fois nos libertés et notre sécurité.** Elle causera des violences pour la population (partie A) sans même pouvoir repousser les menaces qu'elle prétend combattre (partie B).

A. Effets négatifs sur la sécurité

La VSA pose trois menaces pour la sécurité de la population : elle met en danger les **populations qui sont déjà les plus vulnérables** (1), elle favorise structurellement les **comportements violents** de la police contre la population (2), elle offre au pouvoir exécutif une puissance telle qu'**aucun contre-pouvoir** ne pourra en empêcher les abus (3).

1. Mise en danger des populations les plus vulnérables

Comme tout système de surveillance de l'espace public, la VSA surveillera en priorité **les personnes qui passent le plus de temps en extérieur** - les personnes qui, par manque de ressources, n'ont pas ou peu accès à des lieux privés pour sociabiliser ou pour vivre. De plus, la VSA détecte des comportements d'autant plus efficacement qu'elle a pu s'entraîner à partir d'une grande quantité de séquences d'images représentant une même action. Ainsi, les comportements les plus efficacement détectés seront ceux que l'on rencontre le plus souvent dans la rue et les transports - les comportements typiques des populations qui y passent le plus de temps, peu importe que ces activités soient licites ou illicites.

---

1 Voir les villes recensées sur https://technopolice.fr/villes/
2 *« Safe City » de Marseille : on retourne à l'attaque* s https://www.laquadrature.net/2020/12/10/safe-city-de-marseille-on-retourne-a-lattaque/
3 Plus d'information sur la page https://technopolice.fr/marseille/
4 *Lire « Les Suresnois·es : nouveaux cobayes de la technopolice »* https://technopolice.fr/blog/les-suresnois%C2%B7es-nouveaux-cobayes-de-la-technopolice/
5 Plus d'information sur la page https://technopolice.fr/roubaix/

Ce sont précisément ces comportements que les fournisseurs de VSA mettent en avant[6] : maraudage, mendicité, réunions statiques. C'est le mode de vie des populations précaires ou populaires qui sera visé en priorité, alors qu'il ne constitue quasiment jamais un délit ou un crime. La VSA jouera le rôle de **contrôle au faciès automatisé** basé sur des critères sociaux, permettant de multiplier les alarmes sonores ou les contrôles humains et d'exclure une partie de la population de l'espace public, détériorant encore davantage leur sécurité - qu'il s'agisse de dégrader[7] leur cadre de vie ou de les éloigner de l'accès aux soins et aux autres services publics.

La focalisation de la VSA sur les populations les plus pauvres n'est pas le simple « effet de bord » d'une technologie immature qui aurait encore quelques « biais ». Au contraire, la VSA est précisément vendue comme permettant de lutter contre des comportements définis comme « anormaux » qui, bien qu'étant parfaitement communs et « normaux » pour une large partie de la population, **permettent de dénigrer les populations** qui adoptent ces comportements. Ainsi, la VSA est autant un outil d'exclusion sociale qu'un outil de propagande politique, dont l'effet sera d'installer le sentiment que certaines populations (choisies arbitrairement par les fournisseurs de VSA et leurs clients) ne sont pas « normales » et doivent être exclues de l'espace public.

2. Déshumanisation de la population

La VSA renforce la distance qui sépare la police de la population. Cette distance est d'abord physique : l'interaction passe par des écrans et ne se réalise que dans une seule direction. La distance est aussi intellectuelle : les agents n'ont plus à comprendre, à évaluer ou à anticiper l'action des autres humains quand une machine le fait à leur place[8] . Déresponsabilisée, déshumanisée, la police est réduite à un outil d'action mécanique sur les corps, **détachée de l'empathie et de la considération sans lesquelles les violences policières ne peuvent qu'exploser.** Cette même empathie sans laquelle encore davantage de personnes auraient perdu la vie face aux pires crimes commis par la police (tel que notamment documenté[9] pour la période de collaboration nazie).

De façon plus diffuse, cette mise à distance technologique accompagne **une politique générale d'austérité**. La collectivité assèche ses dépenses d'accompagnement et d'aide aux individus pour ne plus financer que leur gestion disciplinaire. Dans un courrier à la CNIL, la région PACA défendait l'expérimentation de la reconnaissance faciale aux abords de deux lycées en affirmant que ce projet constituait « *une réponse au différentiel croissant constaté entre les exigences de sécurisation des entrées dans les établissements et les moyens humains disponibles dans les lycées, dans le cadre des plans successifs de réduction des effectifs dans la fonction publiqu*e ». Le personnel encadrant, soucieux et à l'écoute, est remplacé par des machines dont le seul rôle est d'ouvrir et de fermer des accès. Ou encore à Nîmes, où la métropole a ponctionné[10] presque 10 millions d'euros sur le budget d'investissement « eau » pour les dépenser à la place dans l'achat d'un logiciel de Détection Automatique d'Anomalie en temps réel.

---

6 Par exemple, la RATP a récemment expérimenté dans la salle d'échange du RER des Halles un système pour repérer les personnes statiques pendant plus de 300 secondes. https://www.institutparisregion.fr/fileadmin/NewEtudes/000pack2/Etude_2310/NR_833_web.pdf

7 L'exclusion par la surveillance s'ajoute aux politiques d'urbanisme et d'aménagement urbain déjà déployées contre les populations précaires et populaires. Lire notamment cet article du Bondy Blog : https://www.bondyblog.fr/societe/dans-les-quartiers-populaires-le-tout-securitaire-contamine-jusquau-mobilier-urbain

8 Voir Gregoire Chamayou. "*Théorie du drone*", 2013. L'auteur revient notamment sur la perte d'empathie entraînée par la distance entre le pilote de drone et ses cibles.

9 En plus des divers initiatives individuelles de policiers pendant l'occupation, le cas de la rafle manquée de Nancy illustre comment l'empathie d'un groupe de policiers a sauvé des centaines de personnes, voir https://fr.wikipedia.org/wiki/Rafle_manqu%C3%A9e_de_Nancy

10 Sciences Critiques, «*À Nîmes, la reconnaissance faciale dévoile son vrai visage* » https://sciences-critiques.fr/a-nimes-la-reconnaissance-faciale-devoile-son-vrai-visage/

La vidéosurveillance algorithmique accentue la déshumanisation du contrôle social qui était déjà une critique[11] faite à la vidéosurveillance dite classique. Cette course sans fin s'inscrit dans la fuite en avant technologique générale qui anime à la fois **l'effondrement des services publics et le désastre[12] écologique en cours**.

C'est aussi la population qui est déshumanisée : elle est utilisée comme cobaye[13] pour entraîner les algorithmes. Non content de voir les habitants des villes comme une masse de données à rentabiliser pour le compte d'entreprises de mort, les populations permettent malgré elles de rendre le logiciel plus performant et donc de l'exporter sur le marché international de la surveillance. Par exemple, la multinationale Idémia, affine ses dispositifs de reconnaissance faciale aux aéroports français avec les dispositifs PARAFE ou MONA pour ensuite vendre[14] des équipements de reconnaissance faciale à la Chine et participer à la surveillance de masse et le génocide Ouïghour.

3. Effacement des limites contre les abus de la police

Aujourd'hui, le nombre limité d'agents de police contraint celle-ci à concentrer une large part de ses ressources sur ses missions les plus importantes et les plus légitimes (crimes, violences aux personnes). Elle ne dispose ainsi que d'un temps et de ressources limitées pour poursuivre des activités peu légitimes (contre les populations vulnérables, contre les manifestants) ou qui constituent des abus de son pouvoir (répression d'opposants politiques, persécution de minorités).

Demain, **la VSA promet d'effacer cette limite matérielle** en décuplant les capacités opérationnelles de la police pour poursuivre les missions de son choix, que ces missions soient peu légitimes ou qu'elles constituent des abus. Par exemple, s'il est aujourd'hui extrêmement coûteux de détecter en manifestation l'ensemble des pancartes critiquant le gouvernement, la VSA promet à terme de rendre la chose triviale (facilitant les interpellations sur place ou, couplée à la reconnaissance faciale, permettant de poursuivre en masse les opposants trop expressifs). De même, si le suivi visuel d'opposants politiques implique aujourd'hui des moyens humains si importants que ces opérations ne peuvent rester qu'exceptionnelles, la VSA rend la chose triviale en permettant de suivre, à coût quasi-nul, une personne sur l'ensemble des caméras d'une ou plusieurs villes.

Ce changement d'échelle transforme considérablement la manière dont les pouvoirs de police sont exercés. D'une action précise répondant à des « besoins » pouvant être débattus démocratiquement, nous assistons à l'apparition d'une police omnisciente disposant de la capacité de surveiller et d'agir sur l'ensemble de la population. Avec la VSA, les 250 000 policiers et gendarmes actuels verraient leur autorité atteindre celle qu'auraient eu des millions d'agents non-équipés de telles technologies. De quoi atteindre le ratio police/population typique des États policiers.

Cette multiplication considérable des capacités de la police ne sera **nullement compensée par une multiplication équivalente des capacités de contrôle de ses contre-pouvoirs**. Dès aujourd'hui, l'installation des équipements de VSA se fait à un rythme bien trop important pour que la CNIL ou que des associations comme la nôtre puissent en prendre connaissance à temps et avec suffisamment de détails. Demain, la situation sera encore plus dramatique concernant l'utilisation quotidienne de ces systèmes : aucune autorité, aucun juge, aucun parlement ne pourra vérifier que chacune des innombrables détections réalisées chaque jour ne contribue pas à un abus de pouvoir. **Personne ne pourra vérifier que la VSA ne permet pas à la police de réduire illégalement les conditions de sécurité de larges parties de la population.**

---

11 Lire l'analyse de Rebellyon https://rebellyon.info/10-ans-de-video-surveillance-10

12 Voir notamment https://www.cairn.info/revue-projet-2016-4-page-93b.html

13 Lire l'analyse du dispositif déployé à Suresnes sur https://technopolice.fr/blog/les-suresnois%C2%B7es-nouveaux-cobayes-de-la-technopolice/

14 Plus d'informations sur https://technopolice.fr/idemia/

En plus des risques d'abus policiers, ce changement d'échelle dans la surveillance de l'espace public contribue à criminaliser un nombre croissant de comportements. Ainsi, par exemple, la plupart des logiciels de VSA cherchent à détecter des dépôts d'ordure sauvage[15], le non-port du masque[16], des personnes qui sont statiques[17] dans l'espace public, **sans que ces évolutions aient été actées démocratiquement,** résultant principalement d'initiatives d'entreprises privées.

B. Absence d'effet positif sur la sécurité

Les dégradations dramatiques engendrées par la VSA ne sont compensées par aucun avantage en terme de sécurité. Il s'agit d'un outil inadapté pour lutter contre les violences sur les personnes, que ce soit de par son objet, **l'espace public** (1), ou de par son fonctionnement, **l'automatisation** (2).

Cette double inadaptation repose sur une vision faussée du concept de « sécurité » qui, dans le discours des promoteurs de la VSA, se limite à un pur argument marketing déconnecté de la façon dont la population pourrait concrètement protéger sa santé physique et mentale, ses conditions de vie, son logement et ses capacités d'épanouissement.

1. Inadéquation de l'objet surveillé

L'objet de la VSA est l'espace public. Pourtant, pour l'essentiel, ce n'est **pas dans l'espace public que se réalisent les violences sur les personnes**. Tandis que les agressions sexuelles se déroulent presque toujours dans un contexte privé (91%[18] sont perpétrées par une personne connue de la victime), la grande majorité des homicides, en excluant les conflits entre criminels, interviennent eux aussi en dehors de la voie publique[19].

Cette inadéquation entre l'objet surveillé et la finalité poursuivie est au cœur des nombreuses évaluations qui, depuis une décennie, **concluent unanimement à l'inefficacité de la vidéosurveillance classique** (voir notamment le rapport de la Cour des compte[20], du LINC[21] et d'autres chercheurs[22]).

Ce décalage est accentué en matière de VSA qui, pour fonctionner, doit s'entraîner sur un grand nombre de séquences vidéos représentant les comportements à détecter. Or, les violences sur les personnes sont beaucoup moins nombreuses dans l'espace public que de simples actes de dégradations, de maraudage ou de mendicité. Dès lors, l'algorithme aura **beaucoup moins d'occasions de s'entraîner à détecter des actes de violences sur les personnes** et les détectera beaucoup moins efficacement que d'autres actes plus anecdotiques (dont la surveillance, comme vu précédemment, dégradera les conditions de sécurité des populations les plus vulnérables).

15 Lire sur https://www.nicematin.com/environnement/quand-lintelligence-artificielle-traque-les-depots-sauvages-a-nice-697778
16 Lire sur https://www.journaldunet.com/economie/services/1492433-datakalab-la-start-up-qui-detecte-le-port-du-masque-pour-la-ratp/
17 Lire sur https://www.institutparisregion.fr/fileadmin/NewEtudes/000pack2/Etude_2310/NR_833_web.pdf
18 Statistiques officielles disponibles sur https://arretonslesviolences.gouv.fr/je-suis-professionnel/chiffres-de-reference-violences-faites-aux-femmes
19 Voir les statistiques pour la région parisienne entre 2007 et 2013, graphique 25 https://www.ihemi.fr/sites/default/files/publications/files/2019-12/ga_35_0.pdf
20 Rapport sur les polices municipales, octobre 2020 disponible sur https://www.ccomptes.fr/system/files/2020-11/20201020-rapport-polices-municipales_0.pdf
21 Etude sur la vidéosurveillance dans les villages, novembre 2021 https://linc.cnil.fr/fr/comment-la-videosurveillance-se-developpe-t-elle-dans-les-villages
22 Voir la récente étude Guillaume Gormand commandée par le CREOGN https://www.aefinfo.fr/depeche/663759-pour-le-chercheur-guillaume-gormand-critiquer-la-videosurveillance-c-est-s-attaquer-a-une-religion

2 Inadéquation de la méthode

La prévention des violences sur les personnes repose sur un travail humain et social : accompagnements personnalisés, soins, enquêtes de terrain, analyses sociologiques, réduction des inégalités ou même simplement présence sur le terrain. Ce travail humain a un coût nécessairement conséquent et déjà largement sous-investi, particulièrement dans les zones du territoire ou la précarité est la plus élevée.

À l'inverse, la VSA, probablement moins chère à court terme, n'est capable que de détecter certaines infractions (et parmi les moins graves), sans être capable d'en traiter les causes plus profondes en amont. Une façon de donner l'illusion de traiter les symptômes, sans rien changer sur le long terme.

C'est sans doute là que se trouve l'un des rares avantages de la VSA : offrir aux élus en manque de projet politique enthousiasmant un discours qui fera illusion à court terme. Ce discours est d'autant plus séduisant pour les élus que l'industrie de la VSA a préparé depuis plusieurs années les bons éléments de langage et l'imaginaire suffisamment confus pour espérer tromper le public. Sont décrits comme « **anormaux** » des comportements parfaitement banals mais typiques des populations les moins riches. Est présenté comme « **sécurité** » un objectif qui a bien plus à voir avec la « propreté » de la ville et la « sécurité » des biens qu'avec celle des personnes. Est dite « **augmentée** » ou « **intelligente** » une surveillance policière qui, au contraire, sera « réduite » à de pures tâches mécaniques et défaite de toute l'empathie et de toute la considération qui font l'intelligence humaine.

II. Un cadre juridique actuellement suffisant

Afin de justifier son projet de position, la CNIL estime que les différents usages de la VSA nécessitent d'être hiérarchisés en fonction de leur dangerosité pour les droits et libertés puis d'être encadrés plus ou moins strictement en fonction de cette dangerosité.

Pourtant, l'ensemble de ces usages est déjà suffisamment encadré par les textes en vigueur et il n'apparaît pas nécessaire de créer une loi spéciale pour les technologies de VSA.

En effet, le cadre juridique existant (RGPD, Directive Police/Justice, Loi Informatique et Libertés) prévoit déjà des règles permettant de limiter ou interdire les atteintes aux libertés engendrées par l'usage de ces technologies et s'opposer aux risques pointés par la CNIL et exposés ci-avant. Contrairement à ce qu'affirme la CNIL, les dispositions prévues par ces textes fournissent des garanties suffisantes pour limiter la dangerosité de ces traitements algorithmiques dès lors qu'il s'agit systématiquement de données biométriques dont la définition est particulièrement large (A) et auxquelles sont associées un régime de protection efficace grâce à un contrôle de proportionnalité renforcé (B). Refuser de mettre en œuvre cette protection pour en chercher une nouvelle reviendrait à changer totalement le paradigme du droit des données personnelles et à affaiblir la protection des libertés des personnes (C).

A. Une large définition des données biométriques

L'article 4§14 du RGPD et l'article 3§13 de la Directive Police/Justice définissent les « données biométriques » comme « *les données à caractère personnel résultant d'un* ***traitement technique spécifique*** *(1), relatives aux* ***caractéristiques physiques, physiologiques ou comportementales*** *d'une personne physique (2), qui permettent ou confirment son* ***identification unique*** (3) ».

1. Traitement technique spécifique

Concernant la VSA, les moyens et modalités de traitement incluent tout type d'algorithme ou programme informatique appliqué aux flux vidéos afin d'isoler, caractériser, segmenter ou encore rendre apparente une information relative à une personne physique filmée ou à extraire du flux vidéo, même a posteriori, des données biométriques de cette personne. Chaque fois, ces opérations sont spécifiques en ce qu'elles poursuivent un objectif spécifique (isoler une personne de façon unique ; voir ci-après) et interviennent en addition du traitement général qui consiste à filmer l'espace public.

2. Caractéristiques physiques, physiologiques ou comportementales

Concernant la VSA, les informations **physiques ou physiologiques** peuvent se rapporter au corps d'une personne filmée au sens large, tels que des visages, des silhouettes ou toute caractéristique isolée du corps, telle la couleur des cheveux, la couleur des yeux, la forme du visage, la taille, le poids, l'âge.

Les données **comportementales** visent toute information relative à l'action du corps dans l'environnement et l'espace. Pourront être qualifiés de biométriques un vêtement ou accessoire porté par la personne à un instant T, un geste, une expression d'émotion, une direction de déplacement, une position dans l'espace et le temps (assis, debout, statique, allure de la marche...).

3. Identification unique

Dans ses lignes directrices relatives au traitement des données personnelles par appareils vidéo[23], le Comité européen pour la protection des données (CEPD) apporte des précisions quant à cette notion d'identification unique. Celle-ci n'**implique pas nécessairement de révéler l'état civil d'une personne** mais, plus largement, de **pouvoir individualiser une personne** au sein d'un groupe ou de l'environnement filmé. En effet, pour le Comité « s*i un responsable du traitement souhaite détecter une personne concernée q****ui pénètre à nouveau dans l'espace surveillé*** *ou dans une autre zone (par exemple, pour projeter une publicité personnalisée continue), la finalité* ***serait alors d'identifier de manière unique une personne physique****, ce qui signifie que l'opération relèverait d'emblée de l'article 9. ».*

Le CEPD donne ainsi l'exemple suivant : *« **Dès lors que le système se fonde sur l'analyse de caractéristiques physiques pour détecter des personnes spécifiques qui entrent dans le champ de la caméra (comme les visiteurs d'un centre commercial) et les suivre, il constitue une méthode d'identification biométrique, car il vise la reconnaissance par l'utilisation d'un traitement technique spécifique. »*** (Lignes directrices sur les vidéos contenant des données personnelles 3/201, version 2.0, point 82 p. 19).

Concernant la VSA, l'objectif principal des opérations demandées aux systèmes de VSA est de réunir des éléments concernant une personne physique (couleur des habits, position, direction, comportement) afin de produire un ou deux des effets suivants : **reconnaître** cette personne (a) et/ou **diriger une action ciblée** sur cette personne (b).

a) Reconnaissance

Afin de détecter un comportement qui s'étend ou se répète dans le temps (tels que le maraudage, la mendicité, une course, une chute, etc.) le système de VSA doit distinguer en continu une même personne sur plusieurs images du flux vidéo. Il doit être capable de la « reconnaître » d'une image à l'autre, sans quoi le comportement ne pourrait être caractérisé. Pour ce faire, le système attribue à la personne une identité unique qui n'est pas son état civil mais se compose de l'empreinte numérique d'une ou plusieurs de ses caractéristiques physiques, physiologiques ou comportementales.

De plus, une fois que le système de VSA a détecté un comportement (que ce comportement soit instantané ou non, d'ailleurs), il va généralement chercher à le signaler aux agents humains en encadrant la personne concernée sur leur moniteur vidéo. Cette simple opération, consistant à isoler une personne de façon graphique et unique sur différentes images, implique aussi que le système de VSA confère à la personne une identité unique composée des différentes caractéristiques qui permettent de la « reconnaître » sur le flux vidéo.

La fonction de « reconnaissance » est probablement la plus flagrante concernant un des usages classique de la VSA cité par la CNIL dans son projet : le suivi d'une personne dans la rue, notamment à partir de plusieurs caméras. Ici, le système capture d'abord une première image de la personne, qui n'est alors pas « connue » de lui. À partir de cette première image, il extrait l'empreinte de différentes caractéristiques propres à la personne afin lui conférer une identité unique. Cette identité unique lui permet ensuite de « reconnaître » la personne sur les images prises ultérieurement, notamment par d'autres caméras.

23 Lignes directrices 3/2019 adoptées le 29 janvier 2020 https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_fr.pdf

b) Action ciblée

La finalité globale des systèmes de VSA n'est pas de détecter des comportements mais de permettre à des agents humains de réaliser certaines actions spécifiques en réaction à ces comportements. Pour de nombreux usages de la VSA, cette finalité « finale » consiste à réprimer, éloigner ou mettre en garde les auteurs des comportements jugés indésirables.

Pour ce faire, les agents doivent être capables d'identifier chaque personne de façon unique parmi les nombreuses autres personnes présentes sur les lieux où le comportement détecté est survenu. Concrètement, le système de VSA et/ou les agents qui consultent les flux vidéo doivent transmettre aux agents de terrain une série de caractéristiques physiques, physiologiques et comportementales qui leur permettront de « reconnaître » de façon unique la personne afin d'exercer sur elle l'action ciblée appropriée.

Par exemple, un agent de terrain pourrait recevoir l'ordre de contrôler le titre de transport d'un homme d'une trentaine d'années portant une capuche noire et des chaussures rouges et que le système de VSA a détecté comme venant de dessiner sur le mur d'une rame de métro. Dans ce contexte, le système de VSA a transmis à l'agent les informations nécessaires pour que celui-ci puisse identifier de façon unique la personne ayant réalisé tel comportement afin d'exercer sur elle une action ciblée. Sans cette identification, aucune action n'est possible.

À noter que, dans bien des cas, l'action ciblée consiste directement au relevé de l'état civil de la personne. Dans ce cas, la démonstration est immédiate : la finalité du système de VSA est de collecter l'état civil des personnes concernées.

En conclusion, chacune des deux fonctions de la VSA (reconnaître et exercer une action ciblée) implique l'identification unique d'une personne, et ce peu importe que ces deux fonctions soient réalisées de façon conjointe ou non (par exemple, le comptage statistique implique de « reconnaître » chaque auteur du comportement ciblé afin d'en dénombrer les occurrences, même si aucune action ciblée n'est prise sur chaque personne ; de même, l'interpellation d'une personne à partir d'une alerte VSA implique systématiquement une identification unique de la part des agents humains de terrain, ce qui ne dépend pas du fonctionnement interne du système de VSA).

L'analyse de la définition de données biométriques à travers la caractérisation de ces trois éléments permet de qualifier juridiquement l’ensemble des dispositifs de VSA filmant des personnes physiques de **traitements de données biométriques**

Contrairement à ce qu'affirme la CNIL, les cas d'usages décrits dans son projet de position (§2.2.3) doivent relever de cette qualification. L'exclusion par la CNIL de ces traitements dans l'objet de la consultation (§1.3), et notamment l'exclusion de la reconnaissance faciale n’apparaît alors absolument pas justifiée. Opérer une séparation entre les deux technologies alors qu'elles relèvent du même régime juridique aurait pour incidence de créer une différence de perception dans la société et de faciliter le développement de la vidéosurveillance automatisée, alors qu'elles présentent des dangers aussi importants et des potentiels de surveillance de masse au moins équivalents.

B. Une protection suffisante des données biométriques

L’article 9 du RGPD et l’article 10 de la Directive Police/Justice interdisent le traitement des données sensibles, parmi lesquelles les données biométriques, compte tenu de l’importance des dangers créés pour les droits et libertés.

Ces textes prévoient toutefois un nombre limité d'hypothèses dans lesquelles ces traitements peuvent exceptionnellement être autorisés. L'analyse de ces exceptions permet de constater que les dispositifs de VSA peuvent déjà être suffisamment limités et encadrés, que ce soit par le RGPD (1) ou la Directive Police/Justice (2).

1. Encadrement par le RGPD

Le RGPD encadre les traitements à des fins non-policières et, en ce qui concerne la VSA, l'ensemble des usages par le secteur privé tel que décrit par la CNIL dans son projet de position, qui consistent principalement en des actions commerciales ou publicitaires. Si, en matière de VSA, les exceptions prévues par le RGPD ne sont pas valables (a), de tels traitements seraient, quand bien même, systématiquement disproportionnés (b).

a) Aucune exception valable

Les exceptions pour lesquelles les traitements de données biométriques peuvent être mis en œuvre sont prévues à l'article 6 de la loi Informatique et Libertés qui renvoie à l'article 9, 2, du RGPD. Or, très peu de ces bases légales pourraient justifier l'utilisation d'un système de VSA à des fins non-policières, en l'occurrence dans un but purement commercial ou économique.

Le CEPD rappelle qu'il est « *important de noter que les* ***exceptions énumérées à l'article 9 ne permettraient probablement pas de justifier le traitement de catégories particulières de données par vidéosurveillance****. Plus précisément, les responsables du traitement de données obtenues au moyen de la vidéosurveillance ne* ***peuvent pas se prévaloir*** *de l'article 9, paragraphe 2, point e), qui autorise les traitements portant sur des données à caractère personnel* ***manifestement rendues publiques par la personne concernée****. Le simple fait d'entrer dans le champ de la caméra ne présuppose pas que la personne concernée a l'intention de rendre publiques des catégories particulières de données la concernant »*[24]*.*

Le consentement, exercé dans les conditions de l'article 4 et 7 du RGPD, ne pourra jamais être recueilli pour permettre le traitement de données de toutes les personnes situées dans un espace public filmé par un dispositif de VSA. Il importe peu que le droit d'opposition puisse être effectivement exercé ou non dès lors que le consentement ne peut jamais être valablement donné en amont. Cette base légale doit donc également être écartée.

b) Disproportion systématique

Ensuite, dans l'hypothèse improbable où une exception serait fondée, ce traitement devrait répondre aux exigences de proportionnalité du RGPD, rappelées par la CNIL dans son projet de position, avec au premier chef desquelles l'exigence de la nécessité du traitement. La CNIL s'était penchée, dès 2020[25], sur les critères permettant de satisfaire cette exigence dans le cadre de la VSA. Doivent ainsi être prises en compte « *l'absence de moyens moins intrusifs pour les droits et libertés des personnes concernées permettant d'atteindre les finalités envisagées* », « *l'importance des données traitées* » ou encore les « r*emontées d'informations aux responsables de traitement* ».

L'exigence de ce contrôle de la nécessité est également clairement rappelée par le CEPD dans ses lignes directrices : il « *importe* ***de ne pas recourir systématiquement à la vidéosurveillance lorsqu'il existe d'autres moyens d'atteindre la finalité poursuivie****. Sinon, nous risquons de voir évoluer nos normes culturelles de telle sorte que nous serons amenés à accepter un niveau insuffisant de protection de la vie privée.* » (§5).

Dans le cadre des utilisations commerciales et non-policières de la VSA, il est difficile de croire que d'autre moyen moins intrusifs ne pourraient être mis en œuvre pour faire parvenir de la publicité à

24 Paragraphe 70 des lignes directrices précitées

25 Voir https://www.cnil.fr/fr/cameras-dites-intelligentes-et-cameras-thermiques-les-points-de-vigilance-de-la-cnil-et-les-regles

des consommateurs ou leur vendre des produits, puisque cela est le cas depuis des dizaines et dizaines d'années par des moyens « classiques » excluant tout profilage intrusif dans l'espace public.

La mise en balance exigée par le contrôle de proportionnalité permettra en pratique de limiter et exclure tout diapositif de VSA abusif puisque l'atteinte à la vie privée engendrée par le traitement de données biométrique ne pourra être que très rarement, voire jamais, évaluée comme strictement nécessaire pour atteindre l'objectif poursuivi.

En conclusion, les dispositions du RGPD permettent déjà de limiter les usages commerciaux de ces technologies, et notamment ceux visant à instaurer un profilage de consommateurs.

2. Encadrement par la Directive Police/Justice

Les traitements de données personnelles ayant pour finalité la prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces, sont régies par la directive Police/Justice, transposée au titre III de la loi Informatique et Libertés.

Concernant les données sensibles, l'article 88 de la loi n° 78-17 prévoit que « *le traitement (...) est possible uniquement en cas de* ***nécessité absolue****, sous réserve de garanties appropriées pour les droits et libertés de la personne concernée, et soit s'il est autorisé par une disposition législative ou réglementaire, soit* ***s'il vise à protéger les intérêts vitaux d'une personne physique, soit s'il porte sur des données manifestement rendues publiques par la personne concernée*** ».

Ici encore, aucune des exceptions à l'interdiction de principe ne semble valable (a) et, quand bien même, le critère de nécessité absolue ne serait jamais satisfait (b).

a) Aucune exception valable

Les exceptions justifiant de tels traitements sont ici bien plus limitées que dans le cadre d'utilisation non-policières dans la mesure où les risques pour les personnes sont bien plus graves (violences policières, exclusion sociale, enfermement).

D'une part, les observations du CEPD quant aux « données manifestement rendues publiques » citées ci-avant trouvent également et évidemment à s'appliquer à cette disposition, pour exclure cette base légale comme justification de dispositif de VSA mis en œuvre dans l'espace public.

D'autre part, la protection des intérêts vitaux d'une personne ne correspond pas aux cas d'usage de la VSA présentés par la CNIL ou observés dans la pratique. En outre, si cet objectif faisait partie des motifs de déploiement d'un tel système de surveillance, le contrôle de proportionnalité exigé par la loi ne serait jamais satisfait au regard du déséquilibre entre cette finalité et l'atteinte aux droits engendrée.

b) Disproportion systématique

Si une exception était justifiée, le contrôle de proportionnalité serait renforcé dans le cadre policier : le traitement de données biométriques n'est en effet possible qu'en cas de **nécessité absolue.** Cela signifie qu'**aucun autre moyen ne doit permettre d'atteindre l'objectif poursuivi**.

Ce contrôle de proportionnalité n'est pas une nouveauté et la CNIL l'a elle même efficacement mis en œuvre pour réguler des usages de VSA ces dernières années..

Dans une affaire concernant l'installation de portiques de reconnaissance faciale dans deux lycées, la CNIL a déjà souligné qu'un « *traitement de données [sensibles] doit être proportionné, en termes d'impact pour les droits et libertés des personnes, par rapport à la finalité qu'il poursuit et ne porter que sur des données "nécessaire" pour atteindre cette finalité. Il incombe d'ailleurs au responsable de traitement d'évaluer la nécessité et la proportionnalité du traitement envisagé en tenant le plus grand compte de la nature des données traitées, du contexte de sa mise en œuvre et des risques qu'il représente pour les droits et libertés des personnes concernées* » (courrier adressé le 25 octobre 2019 au président de la région Provence-Alpes-Côte d'Azur par la CNIL[26]). Elle précisait qu'en l'espèce la finalité de sécurisation et de fluidification des entrées au sein des lycées « ***peut incontestablement être raisonnablement atteinte par d'autres moyens*** ». Elle en déduisait que « *les dispositifs de reconnaissance faciale envisagés [. . .] ne sont pas conformes aux principes de proportionnalité et de minimisation des données posés, dans la continuité de la loi du 6 janvier 1978, par le RGPD* ».

Dans le cadre d'un avertissement adressé à la ville de Valenciennes[27] sur un système de vidéosurveillance automatisée la CNIL a affirmé qu'« *Il incombe à la commune de Valenciennes de faire la démonstration de l'adéquation et de la pertinence des données traitées dans le cadre de analyse d'impact quelle doit effectuer en application de l'article 90 de la loi « Informatique et Libertés». Cette démonstration doit notamment porter sur chaque catégorie de données traitées dans ce cadre, sur chacune des fonctionnalités des logiciels utilisés et sur leur utilité attendue. Elle doit tenir compte du nombre de caméras actuellement déployées, des considérations ayant détermine leur implantation, ou encore de leur niveau d'efficacité connu à ce jour.* ***L'absence alternative moins intrusive doit également être documentée*** *Ainsi, en l'état, la* ***nécessité des traitements d'analyse assistée des images n' apparaît pas établie*** *au regard des finalités poursuivies.* »

Ce contrôle de nécessité est également mis en œuvre par les juridictions.

Par exemple, le Conseil d'État a utilisé un tel contrôle de nécessité absolue lors de son examen de l'urgence de l'atteinte aux droits induite par l'utilisation de drones de vidéosurveillance au cours de manifestations :

« *Eu égard au nombre important de personnes susceptibles de faire l'objet des mesures de surveillance litigieuses et à l'atteinte qu'elles sont susceptibles de porter à la liberté de manifestation et alors que l****e ministre n'apporte pas d'élément de nature à établir que l'objectif de garantie de la sécurité publique lors de rassemblements de personnes sur la voie publique ne pourrait être atteint pleinemen****t, dans les circonstances actuelles, en l'absence de recours à des drones, la condition d'urgence doit être regardée comme remplie.* » (Conseil d'État, 446155, lecture du 22 décembre 2020, §11).

Ce mécanisme a aussi été efficacement mobilisé pour des dispositifs de vidéosurveillance « classique » et non biométrique. Dans un arrêt du 9 novembre 2018, la Cour administrative d'appel de Nantes a ainsi rappelé que « *la mise en œuvre de tels systèmes de surveillance doit être assortie de garanties de nature à sauvegarder l'exercice des libertés individuelles. Dès lors leur autorisation suppose qu'une telle mesure soit* ***nécessaire et proportionnée à la préservation de l'ordre public****.* »[28]

Pour juger que le dispositif n'était en l'espèce pas nécessaire, la Cour a estimé que « *si les caméras implantées dans certains sites particuliers, tels la gare ou le bâtiment " Les Carmes ", aux abords*

---

26 Courrier révélé par Mediapart https://www.mediapart.fr/journal/france/281019/la-cnil-juge-illegale-la-reconnaissance-faciale-l-entree-des-lycees

27 Avertissement publié par Mediapart https://www.mediapart.fr/journal/france/010821/videosurveillance-valenciennes-et-son-modele-de-safe-city-hors-la-loi

28 CAA de Nantes, Arrêt du 9 novembre 2018, n°17NT02743 disponible sur https://www.legifrance.gouv.fr/affichJuriAdmin.do?idTexte=CETATEXT000037829899

de la " chapelle bleue " et de l'entrée de la médiathèque, peuvent être regardées comme obéissant aux finalités de protection des bâtiments publics et de leurs abords ou de régulation des flux de circulation, d'autres caméras, notamment installées aux abords des écoles ou à proximité des commerces, bars ou autres établissements recevant du public, ***sans qu'il soit établi, par les statistiques relatives à la délinquance dans la commune, que ces lieux seraient particulièrement exposés à des risques d'agression, de vol ou de trafic de stupéfiants****, n'apparaissent pas justifiées par les finalités auxquelles elles doivent correspondre » et que « le dispositif autorisé, qui s'étend sans justification légale à presque tous les principaux lieux de vie de la commune,* ***apparaît disproportionné au regard des nécessités de l'ordre public*** ».

Le contrôle de nécessité absolue est donc aujourd'hui un mécanisme juridique documenté et efficace pour interdire l'utilisation abusive des technologie par la police dans l'espace public.

En conclusion, l'exposé ci-dessus démontre que le cadre juridique actuel permet déjà de répondre aux interrogations posées par la CNIL et d'assurer un niveau de protection élevé des personnes qui seraient potentiellement filmées par les dispositifs de VSA et a fortiori de reconnaissance faciale. Une protection plus effective ne serait atteinte, non pas par de futures règles hasardeuses, mais par une mise en œuvre plus rigoureuse et systématique des dispositions en vigueur auprès des acteurs publics et privés, notamment par la diffusion d'une interprétation entière et protectrice du concept de biométrie, en amont et lors des contrôles, par la CNIL.

C'est pourquoi l'approche préconisée par la CNIL de réguler les usages de façon spécifique en fonction des risques qu'ils posent n'est en aucun cas pertinente et reviendrait à s'éloigner de ce régime général de protection des personnes. Elle doit absolument être rejetée.

C. Contre le changement de paradigme

La CNIL nous invite à réfléchir à « *une loi spécifique, adaptée aux caractéristiques techniques et aux enjeux en cause* » au prétexte que la « *nécessité réelle, en fonction de circonstances précises, doit impérativement être évaluée à un niveau plus général que les collectivités publiques décidant de leur mise en place [...] sans cohérence* ». Ce faisant, la CNIL refuse d'accepter qu'elle puisse déjà (elle comme les juges) évaluer cette nécessité à un niveau plus général que celui des collectivités publiques, et selon des outils et des critères généraux, déjà inscrits dans la loi Informatique et Liberté et le RGPD

L'approche de la CNIL conduirait à s'éloigner de la protection actuelle fondée sur le contrôle de nécessité pour se rapprocher d'une protection, moins forte, fondée sur l'évaluation des risques (A). L'abaissement de ce niveau de protection ne saurait être compensé par les garanties envisagées pour ce faire (B).

Cette approche fondée sur les risques plutôt que la nécessité s'inscrit dans la ligne du projet de règlement 2021/0106 sur l'Intelligence artificielle proposé par la Commission européenne le 21 avril 2021[29]. Peu importe le vecteur législatif, cette méthode doit être rejetée car elle affaiblirait considérablement la protection des citoyens contre la surveillance, le tout au nom de l'innovation technologique, d'intérêts industriels ou bassement électoralistes.

1. L'approche fondée sur les risques

Dans la future législation qu'elle envisage, la CNIL imagine l'adoption de « c*onditions de légalités différenciées en fonctions des objectifs, des conditions de mise en œuvre et des risques* » des dispositifs de VSA. Autrement dit, cette approche fondée sur les risques implique d'autoriser plus

29 Disponible sur https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0020.02/DOC_1&format=PDF

ou moins largement l'usage de certaines technologies en fonction des risques effectifs qu'elles feraient peser sur les droits et libertés de la population.

Par exemple, certaines personnes pourraient imaginer que la reconnaissance faciale de l'ensemble des personnes situées dans l'espace public poseraient des risques plus importants que la reconnaissance d'une partie seulement de la population, ce qui pourrait impliquer d'interdire l'une et d'autoriser l'autre. Cette approche permet de passer au second plan, voir à terme d'arrêter de traiter, la question de la nécessité des traitements qui, pourtant, dans ces deux exemples, fait systématiquement défaut.

Cette approche avait déjà été formellement rejetée au moment de l'adoption du RGPD au regard des faiblesses qu'elle entraînerait pour le droit des personnes. Le G29 était clair : « *les droits accordés à la personne concernée par le droit européen doivent être respectés quel que soit le niveau des risques que ces dernières encourent du fait du traitement des données concerné* »[30] (Traduction libre, §2). « *Les principes fondamentaux applicables aux responsables du traitement doivent rester les mêmes, quels que soient le traitement et les risques pour les personnes concernées*» (Traduction libre, §4).

Dans le droit actuel, avec la notion de « nécessité absolue », **la charge de la preuve repose entièrement sur la personne mettant en œuvre les systèmes de surveillance**. Elle doit démontrer au cas par cas l'impossibilité matérielle de ne pas utiliser ces technologies pour atteindre son but. En face, les populations surveillées bénéficient donc d'**une présomption juridique très forte**. Ces populations n'ont pas à démontrer que cette surveillance leur cause un dommage concret, car cette surveillance est présumée jusqu'à preuve du contraire comme étant contraire aux valeurs défendues par les sociétés démocratiques.

En changeant de paradigme vers une approche fondée sur les risques, cette présomption disparaîtrait, cédant le pas à un équilibre à chercher au cas par cas entre police et population. Cet équilibre **finira toujours en défaveur de la population**. En effet, il est extrêmement difficile de démontrer concrètement les dégâts systémiques causés par la surveillance de masse – c'est bien pour combler cette difficulté que le droit avait posé une présomption en faveur de la population. Au contraire, la police n'aura aucun mal à monter en épingle le moindre fait divers pour laisser miroiter une utilité plus ou moins sérieuse de la VSA.

En conclusion, la CNIL doit revenir sur son projet de position et réaffirmer, dans l'esprit du RGPD, que toute atteinte aux libertés des personnes est illicite par défaut, à moins que sa nécessité absolue pour la population ne soit démontrée. La CNIL doit rappeler le plus fermement possible qu'il ne suffit pas qu'une technologie soit « peu risquée » pour que celle-ci devienne « nécessaire » ni même souhaitable.

2. Des garanties défaillantes

La CNIL, tout comme le projet de règlement IA, envisage que l'autorisation de technologies aujourd'hui interdites pourrait être compensée par certaines garanties à même d'en contenir les risques.

En premier lieu, il faut souligner que, encore une fois, comme pour la question des risques, la présence plus ou moins importante de garanties ne change rien à la nécessité des traitements en cause. Comme pour les risques, mettre en avant la questions des garanties fera passer au second plan, ou exclura sur le long terme, la question de la nécessité. Cette perspective doit être entièrement rejetée.

30 Opinion 14/EN WP 218, 30 mai 2014, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf

En second lieu, même à traiter sérieusement la question des garanties, celle-ci ne résiste pas à l'expérience des faits. Depuis la dizaine d'année que nous mobilisons le droit contre des systèmes de surveillance, force est de constater que les garanties initialement envisagées par la législateur n'ont été que d'une aide très marginale pour protéger la populations contre les pratiques illicites des autorités. Les fois où nous sommes effectivement parvenus à faire interdire une de ces pratiques, la plupart du temps, celle-ci avait déjà été déployée, parfois à grande échelle, et avait donc déjà produit ses effets illicites et nocifs. Les analyses d'impact, les pouvoirs de contrôle de la CNIL, les soi-disant contre-pouvoirs locaux, les droits d'information du public, aucune de ces garanties n'avaient empêché les autorités de violer la loi.

Si nous sommes parvenues à mettre fin à certaines pratiques illégales, c'est avant tout grâce aux dispositions qui définissent les conditions de validité des traitements - il nous suffisait de démontrer que ces conditions, la nécessité en premier lieu, n'étaient pas remplies.

Si l'approche fondée sur les risques devait être adoptée, elle donnerait le signal attendu par l'ensemble des acteurs de la VSA pour déployer massivement et au pas de course l'ensemble de leurs systèmes. Ni la CNIL ni les associations comme la nôtre ne parviendront à prendre connaissance, à évaluer et à contester tous ces systèmes dans la mesure où, même aujourd'hui, nous y échouons encore trop souvent. Rien ne permet de penser que les garanties juridiques envisagées pour demain seraient moins défaillante que celle d'aujourd'hui. Demain comme aujourd'hui, seules les mesures d'interdiction, fondées notamment sur la nécessité, pourront nous protéger.

L'avis commun[31] du Comité européen pour la protection des données (CEPD/EDPB) et du Contrôleur européen pour la protection des données (CEPD/EDPS) sur le projet de règlement sur l'intelligence artificielle reprend l'ensemble de ces conclusions.

L'EDPB et l'EDPS considèrent que l'interdiction de principe des certaines pratiques devient illusoire dès lors que le texte prévoit des exceptions qui, bien qu'entourées de prétendues garanties, « *limitent le champ d'application de l'interdiction dans une mesure telle qu'elle pourrait se révéler dépourvue de sens dans la pratique* » (§28). Les deux autorités en déduisent logiquement, conformément au droit actuel, que doivent être interdites de façon généralisée :

- *« toute utilisation de* ***l'IA en vue d'une reconnaissance automatisée des caractéristiques humaines dans des espaces accessibles au public, tels que les visages, mais aussi la démarche, les empreintes digitales, l'ADN, la voix, la pression sur des touches et d'autres signaux biométriques ou comportementaux, dans tous les contextes****.* » (§32).
- la catégorisation biométrique « ***tant pour les autorités publiques que pour les entités privées*** » c'est à dire « *des systèmes d'IA classant les individus à partir de données biométriques (par exemple, à partir de la reconnaissance faciale) dans des groupes en fonction de l'origine ethnique, du sexe, ainsi que de l'orientation politique ou sexuelle, ou d'autres motifs de discrimination* » sont également visés par la demande d'interdiction (§33).

En conclusion, changer de paradigme en remplaçant l'approche actuelle fondée sur la nécessité par une approche nouvelle fondée sur les risques conduira à présenter comme potentiellement licites des traitements dont l'illégalité ne font aujourd'hui aucun doute. Ce changement de contexte conduira au déploiement massif de systèmes de VSA illicites sans qu'aucune garantie ne puisse en limiter les effets nocifs pour la population. Seule l'interdiction de ces pratiques, telle que permise par le cadre juridique actuel, est à même de protéger la population contre les abus des autorités en matière de surveillance.

31 Avis 05/2021 du 18 juin 2021 https://edpb.europa.eu/system/files/2021-10/edpb-edps_joint_opinion_ai_regulation_fr.pdf