CAMÉRAS DITES « INTELLIGENTES » OU « AUGMENTÉES » DANS LES ESPACES PUBLICS

POSITION SUR LES CONDITIONS DE DÉPLOIEMENT

Juillet 2022

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Sommaire

1. Observations préalables

Depuis quelques années, la CNIL constate une tendance visant à la multiplication des dispositifs de vidéo « augmentée » (ou dite « intelligente »). Ces dispositifs, constitués de logiciels de traitements automatisés d'images associés à des caméras, permettent d'extraire diverses informations à partir de flux vidéo qui en sont issus. Par ce terme, peuvent donc être évoqués les dispositifs de suivi ou traçage, de détection d'événements suspects (par exemple, sauter par-dessus un portique de métro) ou d'objets abandonnés, de caractérisation des personnes filmées (tranche d'âge, genre, comportement, etc.) ou encore permettant l'identification ou la caractérisation des personnes par des traitements de données biométriques (par exemple, la reconnaissance faciale) ou non (caractérisation colorimétrique des vêtements portés). De tels dispositifs sont susceptibles d'être utilisés par tout type d'acteurs, publics comme privés, en particulier dans la rue ou des lieux ouverts au public, pour satisfaire des objectifs divers.

Qu'il s'agisse de vouloir améliorer la sécurité des personnes ou des biens, de mener des opérations de publicité ciblée, ou encore d'effectuer des analyses statistiques de flux de fréquentation, la technologie des vidéos dites « augmentées » est de plus en plus présente. Elle offre de nouvelles perspectives à ses utilisateurs avec une **capacité opérationnelle qui tend à s'accroître au fur et à mesure des avancées réalisées en matière de traitement d'algorithmes dits « d'intelligence artificielle »**[1].

Si le terme « vidéo augmentée » recouvre une grande variété de solutions, **le présent document traite des dispositifs, fixes ou mobiles, déployés dans les espaces publics**[2] **à l'exclusion :**

- **des dispositifs de reconnaissance biométrique** [3], et notamment des dispositifs de reconnaissance faciale qui font l'objet de problématiques et d'un encadrement spécifique déjà évoqués par la CNIL dans une publication de novembre 2019[4] ;
- **des usages des dispositifs de vidéo « augmentée »** :
  - dans des lieux non ouverts au public (par exemple bureaux, réserves ou entrepôts de magasins, etc.) ;
  - dans un cadre strictement domestique ;
  - en temps différé ;
  - détectant des sons ;
  - ou encore à des fins de recherche scientifique au sens du RGPD.

De nombreuses publications en la matière (articles de presse, de recherches, brochures commerciales, guide 2020 de l'association nationale de la vidéoprotection, etc.), ainsi que l'augmentation des demandes de conseil auprès de la CNIL concernant les conditions de développement de ces dispositifs attestent d'une dynamique générale de déploiement de ces derniers un peu partout en France. Une telle dynamique intervient à la faveur **d'intérêts politiques, économiques, industriels et de souveraineté,** soulignés notamment par la stratégie de l'État pour l'intelligence artificielle et le rapport « Villani » de mars 2018[5], ou encore le contrat stratégique 2020-2022 de la Filière « industries de sécurité » du Comité national de l'industrie[6].

On peut notamment mentionner le souhait des autorités publiques de s'équiper de dispositifs toujours plus perfectionnés pour l'exercice de leur mission de sauvegarde de l'ordre public, de protection des populations ou encore d'aménagement des territoires, ou celui des commerçants de vouloir optimiser le pilotage de leur activité et la rentabilité de celle-ci, au moyen d'une connaissance encore plus fine des conditions et caractéristiques de fréquentation de leurs espaces de vente.

---

[1] Sur les récents travaux de la CNIL en matière d'intelligence artificielle, voir https://www.cnil.fr/fr/intelligence-artificielle/ia-comment-etre-en-conformite-avec-le-rgpd

[2] Voies publiques, lieux et établissements ouverts au public.

[3] Dispositifs qui visent à identifier un individu automatiquement et de manière unique à partir de ses caractéristiques physiques, physiologiques ou comportementales conformément aux articles 4(14) et 9.1 du RGPD.

[4] « Reconnaissance faciale : pour un débat à la hauteur des enjeux » sur cnil.fr.

[5] « Donner un sens à l'intelligence artificielle », rapport de Cédric Villani (PDF, 4,4 Mo) sur aiforhumanity.fr.

[6] « Contrat stratégique de la filière industrie de sécurité » (PDF, 6 Mo) sur conseil-national-industrie.gouv.fr.

Si les enjeux pour les acteurs et la légitimité de certains usages ne peuvent être ignorés, ceux-ci doivent être considérés au travers du prisme, essentiel dans toute société démocratique, de la protection des libertés et droits fondamentaux des personnes filmées et analysées par ces dispositifs, et en particulier de la protection de leur vie privée et de leurs données à caractère personnel.

Au-delà d'un simple « prolongement » technique des caméras existantes, ces dispositifs modifient la nature des dispositifs de vidéoprotection « classiques » et posent des questions éthiques et juridiques nouvelles.

À l'heure où les outils se créent et se déploient de façon parfois hétérogène, sur la base d'une multitude d'initiatives locales, en dehors de tout cadre juridique les encadrant spécifiquement, la perspective d'une surveillance et d'une analyse algorithmique permanentes d'espaces publics peut générer ainsi de fortes inquiétudes. En témoignent notamment la mobilisation d'associations et de collectifs citoyens sur le sujet, l'identification de la problématique par les pouvoirs publics français dès la genèse de la technologie (un rapport sénatorial[7] soulignait déjà les risques « vie privée -libertés publiques » associés à l'émergence de tels dispositifs), l'actuel projet de règlement européen sur l'intelligence artificielle et les prises de position récentes d'organisations européennes et internationales (Comité européen de la protection des données[8], Conseil de l'Europe[9] et Haut-Commissariat des Nations unies aux droits de l'homme[10]).

De son côté, la CNIL s'intéresse de longue date à ces évolutions.

Après avoir souligné, en 2017, dans le cadre de ses travaux « études, innovations et prospectives », les problématiques soulevées par le développement des « villes surveillées » (« *safe cities* ») et les enjeux éthiques des traitements algorithmiques et de l'intelligence artificielle, la CNIL a publiquement appelé en septembre 2018 à un débat démocratique sur les nouveaux usages de la vidéo. En juin 2020, elle a lancé une alerte sur la multiplication de certains dispositifs de vidéo « augmentée » dans le cadre de la gestion de la crise sanitaire du COVID-19[11].

Compte tenu de l'ensemble des enjeux attachés au déploiement de ces dispositifs, la CNIL a estimé nécessaire que l'ensemble des parties prenantes aient l'opportunité de s'exprimer et de faire valoir leurs besoins, leurs analyses et leurs alertes en la matière au travers d'une consultation publique qui s'est tenue entre janvier et mars 2022.

À l'issue de cette consultation, elle présente ici sa compréhension, ses réflexions et analyses sur le sujet, d'un point de vue éthique, technique (portrait de la technologie, de ses cas d'usage (2) et des risques qui s'y attachent (3)) **et juridique** (cadre applicable tel qu'il existe actuellement : qu'est-il possible de faire à droit constant, dans quelles conditions et avec quelles garanties ? (4).

Dès lors que la légitimité de certains usages de ces technologies serait actée, la CNIL estime indispensable d'établir un socle de confiance nécessaire à leur implantation et à leur pérennisation. Un cadre juridique clair, qui devrait passer par l'édiction de normes spécifiques, doit permettre de développer des technologies européennes compétitives incarnant des modèles protégeant la vie privée dès la conception (« *privacy by design* »), sur la scène nationale, européenne et internationale. Elle estime tout autant nécessaire de définir collectivement certaines « lignes rouges » à ne pas franchir (comme par exemple des dispositifs de caméras augmentées mettant en œuvre une notation sociale sur la base de l'analyse de comportements dans certains lieux publics).

---

[7] Rapport d'information n° 131 (2008-2009) de MM. Jean-Patrick COURTOIS et Charles GAUTIER, fait au nom de la commission des lois, déposé le 10 décembre 2008 : « La vidéosurveillance : pour un nouvel encadrement juridique » sur senat.fr.

[8] Le Comité européen de la protection des données (CEPD) et le Contrôleur européen de la protection des données ont invité le législateur européen à prévoir, au sein de la proposition de règlement de la Commission européenne sur l' « intelligence artificielle », une interdiction générale concernant aussi bien l'usage de systèmes biométriques aux fins de classer les individus dans des groupes basés sur des critères (genre, orientation sexuelle ou politique, ethnicité, etc.) que l'utilisation de tels systèmes pour déduire des émotions ; voir l'article « Intelligence artificielle : l'avis de la CNIL et de ses homologues sur le futur règlement européen » sur cnil.fr

[9] Conseil de l'Europe, Convention 108, « Lignes directrices sur la reconnaissance faciale », page 5 (PDF, 2,9 Mo) sur rm.coe.int.

[10] « Intelligence artificielle : face aux risques d'atteinte à la vie privée, l'ONU demande un moratoire sur certains systèmes » sur news.un.org.

[11] « La CNIL appelle à la vigilance sur l'utilisation des caméras dites « intelligentes » et des caméras thermiques » et « Caméras dites « intelligentes » et caméras thermiques : les points de vigilance de la CNIL et les règles à respecter » sur cnil.fr.

2. La vidéo « augmentée » : portrait d'une technologie aux multiples usages

Les notions de vidéo ou caméra dite « intelligente » ou « augmentée » sont des concepts protéiformes renvoyant à des technologies d' « intelligence artificielle » dans le domaine de l'analyse d'images ou « vision par ordinateur » pouvant couvrir des usages très variés. Il est donc nécessaire de poser précisément les termes de ces notions et des usages potentiels, afin d'être en mesure d'appréhender les risques induits et de fixer le cadre légal qui leur est applicable.

2.1. Une technologie consistant en une analyse automatisée d'images à partir de caméras vidéo

Le terme de vidéo « augmentée » désigne ici des dispositifs vidéo auxquels sont associés des traitements algorithmiques mis en œuvre par des logiciels, permettant une analyse automatique. Le présent document ne s'intéresse qu'aux caméras « augmentées » analysant les images en temps réel et en continu. Il s'agit de technologie dite de « vision par ordinateur » (« *computer vision* »), qui est une des branches de l' « intelligence artificielle », consistant à munir les systèmes de capacités d'analyse des images numériques, par l'extraction d'informations comme la reconnaissance de formes, l'analyse des mouvements, la détection des objets, etc.

La surcouche logicielle permet de « reconnaître », de façon probabiliste, des objets ou des silhouettes, des attributs, des caractéristiques (typologie d'un véhicule, sexe ou tranche d'âge d'un individu, etc.), ou encore des comportements, des évènements particuliers (regroupement de personnes sur la voie publique, mouvement de foule, déplacement, stationnement d'un véhicule ou d'un individu dans un endroit précis, etc.) déterminés en amont par les concepteurs et utilisateurs.

En pratique, les traitements algorithmiques d'analyse automatisée des images sont soit couplés à des caméras préexistantes de « vidéoprotection » (celles installées dans les espaces publics qui sont autorisées par arrêté préfectoral pour des finalités prévues par le code de la sécurité intérieure), soit spécifiquement déployés avec des dispositifs *ad hoc*.

Même lorsque traitements algorithmiques s'intègrent à des caméras vidéo traditionnelles, le traitement de données qu'ils opèrent change la nature et la portée de la vidéo que nous connaissons depuis plusieurs dizaines d'années[12].

En effet, en permettant à leurs utilisateurs d'obtenir instantanément et de manière automatisée un grand nombre d'informations qui, pour certaines, ne pourraient être détectées par la seule analyse humaine des images, de tels algorithmes **multiplient les capacités des dispositifs vidéo classiques.**

Les dispositifs de vidéo « augmentée » dont il est ici question se distinguent des traitements de données biométriques (et plus spécifiquement des dispositifs de reconnaissance faciale) car les dispositifs de vidéo « augmentée » :

- ne traitent pas toujours les caractéristiques physiques, physiologiques ou comportementales des personnes (par exemple un dispositif de caméra « augmentée » qui va filmer la rue pour identifier les différents usages : passage de voitures, vélos, motos) ;
- n'ont pas toujours pour finalité l'identification unique des personnes concernées, c'est-à-dire leur reconnaissance d'une caméra à une autre (par exemple un dispositif de caméra « augmentée » qui va segmenter les personnes dans un lieu selon leur âge ou encore détecter une bagarre ou des comportements dangereux dans une foule).

Les dispositifs de reconnaissance biométrique conjuguent, quant à eux, toujours ces deux critères. Si la CNIL n'a pas souhaité inclure les caméras augmentées procédant à de la reconnaissance biométrique dans le champ du présent document, c'est parce qu'elles relèvent du régime juridique spécifique des données biométriques (article 9 du RGPD), dont le traitement est en principe interdit, et que les nombreuses

[12] La CNIL et d'autres autorités appellent par ailleurs à mieux évaluer l'efficacité réelle de ces dispositifs, qui se multiplient. Voir les travaux du Laboratoire d'innovation numérique de la CNIL (LINC) : « Les caméras au village – Dynamiques de développement de la vidéosurveillance dans les petites communes françaises » (novembre 2021) sur linc.cnil.fr et le rapport de la Cour des comptes d'octobre 2020 sur les polices municipales (PDF, 4,5 Mo) sur ccomptes.fr, qui pointe la problématique du manque d'évaluation.

interpellations des acteurs sur les conditions de licéité de ces technologies portaient sur des dispositifs non biométriques.

2.2. Des cas d'usages multiples

Le recours à la vidéo « augmentée » peut s'inscrire dans des contextes extrêmement divers, au service d'intérêts aussi bien publics que privés.

Ces dispositifs peuvent, du fait de leurs capacités, s'intégrer dans des lieux de natures très différentes (voie publique, transports publics, centres commerciaux, culturels et sportifs, etc.), avec une couverture géographique, des exigences de densité (quelques caméras ou un réseau très maillé) et des infrastructures très variées (mobile, fixe, embarquée, drone, portable, etc.) pour poursuivre des objectifs divers.

Les questionnements ou initiatives en la matière portés ces derniers mois à la connaissance de la CNIL, notamment par des développeurs d'outils et initiateurs de projets, témoignent de la **multitude des cas d'usage envisageables**. Parmi ceux-ci, on peut par exemple relever :

- **dans le secteur public :**
  - l'exercice de leurs missions de police administrative et judiciaire par des autorités publiques, notamment municipales, via la détection automatisée :
    - de situations permettant de présumer la commission d'infractions (stationnement interdit, circulation en contre-sens, dépôt sauvage d'ordures, etc.) ;
    - ou encore d'évènements « suspects » ou potentiellement dangereux (attroupements d'individus, présence anormalement longue d'une personne dans des lieux et à des moments donnés, expressions faciales, comportements traduisant un état d'angoisse, etc.) ;
  - la régulation des flux de circulation et l'aménagement de leur territoire par des collectivités, dans une logique à la fois sécuritaire, d'optimisation, écologique et économique. Le dispositif permettrait une comptabilisation et une différenciation en temps réel des usages (piétons, camions, vélos, trottinette…), afin notamment :
    - d'identifier et de résoudre d'éventuels conflits d'usage (modification de la signalétique, développement sur la chaussée de voies, pistes réservées à certaines catégories d'usagers, etc.),
    - ou encore d'envisager une revitalisation de certains quartiers par des décisions en matière de commerces, d'évaluer l'impact des investissements réalisés et d'en prévoir de nouveaux ;
  - la détection de bagages abandonnés et le suivi par les exploitants de transports publics à des fins d'intervention par les services de sécurité compétents, des individus les ayant abandonnés ;
  - ou encore la mesure de l'affluence et de la fréquentation des quais du métro ou d'une gare, à des fins de diffusion de messages informatifs dynamiques à l'intention des usagers (zones à éviter, espaces ou itinéraires à privilégier, etc.) ou d'amélioration de la gestion du réseau ;
  - l'évaluation du niveau de respect des règles sanitaires en vigueur (par exemple, mesure du taux de port du masque) à des fins de sensibilisation des usagers ;
- **dans le secteur privé :**
  - la sécurisation des personnes et des biens dans des magasins, salles de concert ou autres établissements recevant du public grâce à la détection de certaines situations ou comportements (port d'objets dangereux, vol à l'étalage ou actes de violence, etc.) ;
  - la mesure de l'audience des panneaux publicitaires sur la base d'un comptage des individus passant à proximité ;
  - la réalisation d'actions de prospection ciblée, individuelle ou collective, au moyen d'une prise en compte des attributs des individus passant près d'un panneau publicitaire (par exemple : sexe, tranche d'âge, etc.) ;

- l'analyse de la fréquentation des enseignes de centres commerciaux à des fins d'amélioration de leur gestion : aménagement, pilotage logistique ou opérationnel, valorisation des espaces et de leurs produits, évaluation de leur attractivité, facturation, etc. tels que :
    - la réorganisation du contenu des rayons en considération des typologies de clients et de leurs déplacements au sein du magasin ;
    - l'ajustement des moyens en personnel ou des actions de nettoyage de façon dynamique ou en fonction des jours / créneaux horaires les plus fréquentés ;
    - l'analyse et la facturation des achats de manière automatisée (magasins dits « autonomes » sans personnel) ;
    - le calcul du prix du bail commercial en raison de la fréquentation du local ;
    - l'appréciation de l'utilité d'un *showroom* physique et de la pertinence des produits exposés ;
    - la modulation des prix des produits en fonction des modes d'interaction avec les têtes de gondole et le comportement d'achat, mis en perspective avec les parcours clients, au sein du centre commercial, etc.

Les dispositifs de vidéo « augmentée » offrent plusieurs avantages techniques : ils permettent, d'une part, d'automatiser l'exploitation des images captées par les caméras, qui était auparavant humaine ; d'autre part, ils offrent une puissance d'analyse de certains paramètres qu'un œil humain ne pourrait pas atteindre. Ce faisant, ils permettent de valoriser des parcs de caméras déjà installés.

Cette liste – non exhaustive – de cas d'usage implique cependant des conditions de traitement de données tout à fait variables, et des impacts différents sur la vie privée des personnes filmées :

- les informations prises en compte ou inférées peuvent être plus ou moins objectives et sensibles ;
- leur traitement peut être plus ou moins intrusif (simple comptage, segmentation des publics sur la base de caractéristiques physiques, analyse comportementale, détection des émotions, traçage ou suivi spatio-temporel des individus, etc.) ;
- leur conservation peut être réalisée sous une forme identifiante plus ou moins longue (anonymisation ou non à bref délai) ;
- enfin, le contrôle laissé aux personnes concernées sur le traitement de leurs données peut être plus ou moins effectif (possibilité ou non de s'y opposer, voire d'y consentir).

Il convient également de souligner que ces technologies peuvent être utilisées sans qu'il y ait traitement de données à caractère personnel (par exemple, un système d'analyse de pièces de monnaie sur un tapis roulant) et ne relèvent alors pas de la compétence de la CNIL.

Dans ce contexte, une appréciation globale de ces dispositifs n'a pas de sens : il convient de les appréhender au cas par cas, en fonction notamment des risques qu'ils comportent pour les personnes concernées.

Leur essor est souvent motivé par les niveaux de performance atteints ces dernières années, , l'adaptabilité de cette technologie à des cas d'usages potentiellement illimités (un capteur vidéo peut être utilisé pour différents usages) et un coût d'exploitation réduit par rapport aux dispositifs vidéo classiques (l'automatisation pouvant permettre d'économiser les coûts salariaux des opérateurs de vidéosurveillance), dans un contexte où la multiplication des caméras installées dans l'espace public en rend l'exploitation en temps réel toujours plus difficile et plus coûteuse en personnel.

2.3. État des lieux industriel et économique du marché de la vidéo « augmentée »

Si la technologie de vidéo « augmentée » existe depuis les années 1980, c'est la puissance atteinte par les microprocesseurs dans les années 2000 qui a permis leur développement pour un coût raisonnable pour les utilisateurs professionnels (quelques milliers d'euros) ainsi que les progrès des performances dans le domaine de la « vision par ordinateur » depuis les années 2010, grâce notamment aux technologies d'apprentissage

automatique (« *machine learning* »). Ces nouveaux usages sont susceptibles de se déployer, notamment dans les espaces où les caméras classiques sont déjà présentes (voie publique, points de ventes, etc.), ces espaces étant eux-mêmes en extension avec l'essor de la vidéoprotection.

Le marché de la vidéo « augmentée » est un marché mondial en croissance rapide, de quelque 7 % par an et estimé à 11 milliards de dollars en 2020[13], **mais aussi très fragmenté.** Il rassemble des grands groupes industriels internationaux, mais également des start-ups innovantes. Les premiers sont historiquement des fabricants de matériels (caméras, enregistreurs), qui intègrent désormais des dispositifs d'analyse d'images. Les secondes se concentrent plus spécifiquement sur le développement de technologies d'analyse automatique des flux vidéo basées sur des algorithmes d' « intelligence artificielle ». Il s'agit d'un marché très hétérogène et très concurrentiel, avec des possibilités de croissance tant organique qu'externe.

On compte aujourd'hui **quatre usages principaux** sur le marché de la vidéo « augmentée » : l'industrie (management de processus dans le cadre de l'industrie dite « 4.0 » logistique), les usages de défense, le domaine dit des « villes connectées » ou « *smart cities* » (surveillance de voie publique, des sites et des infrastructures y compris les usages de mobilité), le commerce de détail (comptage, lutte contre le vol, surveillance des parkings, etc.), auxquels s'ajoute une multiplicité d'autres cas d'usages potentiels ou émergents. Les enjeux en matière de données à caractère personnel se concentrent principalement sur les deux derniers segments. Le marché des caméras « augmentées » pour les usages des particuliers (sécurité et domotique), relève d'un segment différent (et non visé par ce document).

Le marché français est détenu essentiellement par des acteurs étrangers. En 2015, plus d'un tiers des équipements de vidéoprotection installés étaient importés de Chine, mais des acteurs étasuniens, allemands et suédois sont également présents. De fait, si la France dispose de leaders mondiaux en matière de sécurité électronique, gestion des identités d'accès et cybersécurité, elle ne dispose pas encore d'acteurs de cette taille pour ce qui est des équipements vidéo.

De fait, le secteur de la vidéoprotection représentait 1,6 milliard d'euros de chiffre d'affaires en France en 2020 selon l'Association nationale de la vidéoprotection (AN2V), à comparer aux 28 milliards d'euros de chiffre d'affaires pour l'ensemble des industries de sécurité privées.

Les secteurs de la vidéoprotection, vidéosurveillance et des caméras augmentées sont aussi porteurs d'enjeu en matière d'emploi. Le secteur de la vidéoprotection emploie ainsi dans notre pays 12 000 personnes, selon le rapport d'information de l'Assemblée nationale sur les enjeux économiques de la sécurité privée de mai 2021[14].

L'autre enjeu est un enjeu d'innovation industriel. Des solutions de vidéo « augmentée » sont en train d'être développées par deux types d'acteurs : soit des PME ou ETI du secteur de la sécurité, distributeurs ou intégrateurs qui ont fait de la vidéo « augmentée » un axe de développement de leur modèle d'affaires, notamment dans le domaine du commerce de détail ; soit des « jeunes pousses » qui conçoivent des algorithmes d' « intelligence artificielle », notamment dans le domaine de la mobilité et des « villes connectées » (« *smart cities »)*. C'est plutôt cette partie logicielle de la chaîne de valeur de la vidéo « augmentée », avec les créations d'emplois associées, qui est accessible à des innovateurs français, les fabricants de matériel étant le plus souvent situés dans des pays tiers très compétitifs.

3. Une technologie porteuse de risques gradués pour les droits et libertés des personnes

Par leur fonctionnement même, reposant sur la détection et l'analyse en continu et en temps réel des attributs ou des comportements des individus dans un espace ouvert au public, les dispositifs de vidéo « augmentée » présentent, par nature, des risques pour les personnes concernées. L'importance et l'effectivité de ces risques doivent être précisément évaluées afin d'établir les garanties nécessaires et de poser des limites à certains usages de ces dispositifs.

[13] Étude de marché sur le « *machine vision market* » 2021 (en anglais) du cabinet de consultants Marketsandmarkets.com.

[14] https://www.assemblee-nationale.fr/dyn/15/rapports/cion-eco/l15b4194_rapport-information

3.1. D'un risque de surveillance généralisée à un risque d'analyse généralisée ?

Dans un système de caméra vidéo classique, l'image des personnes est visionnée (ou enregistrée) par un nombre limité de personnes situées derrière un écran de contrôle. Ces caméras se limitent à capter et à enregistrer les images pouvant être saisies dans leur champ de vision. En outre, ces images, qui sont rarement visionnées dans leur totalité mais plutôt aléatoirement ou dans le cadre d'une recherche ciblée, ne « disent » rien d'autre que ce qu'en retirent les personnes y ayant accès.

L'intégration de traitements algorithmiques dans ces systèmes vidéo, analysant de manière systématique et automatisée les images issues des caméras, a pour conséquence d'élargir considérablement les informations qui peuvent en être inférées. **Ces nouveaux outils vidéo peuvent ainsi conduire à un traitement massif de données à caractère personnel, y compris parfois de données sensibles**[15].

Les personnes ne sont donc plus seulement *filmées* par des caméras mais *analysées* de manière automatisée afin d'en déduire, de façon probabiliste, certaines informations permettant, le cas échéant, une prise de décisions ou de mesures concrètes les concernant.

Un tel changement ne constitue pas une simple évolution technologique de dispositifs vidéo, mais une modification de leur nature. La CNIL rappelle à cet égard qu'une vigilance particulière doit être accordée à l'égard de la tentation du « solutionnisme technologique » qui consisterait à considérer que les dispositifs de vidéo « augmentée » sont par nature efficaces et permettraient de résoudre de nombreux problèmes.

La CNIL a depuis longtemps pointé le risque d'une surveillance généralisée des individus, induit par la multiplication des dispositifs vidéo. Cette surveillance était toutefois limitée matériellement par les capacités humaines de visionnage des images. Ce risque prend aujourd'hui une nouvelle dimension avec un **risque d'analyse généralisée des personnes** : les dispositifs automatisés offrant un champ, une systématisation et une précision d'analyse impossibles jusque-là pour un humain. Au-delà de créer un phénomène d'accoutumance et de banalisation de technologies de plus en plus intrusives, **ces dispositifs pourraient offrir à leurs utilisateurs la faculté de connaître des éléments nouveaux sur les personnes filmées pour prendre des décisions et des mesures les concernant** (analyser le parcours d'achat d'une personne dans un magasin et en déduire ses goûts et ses habitudes, analyser le visage d'une personne pour en déduire son humeur et afficher une publicité ou des promotions en conséquence, etc.).

Ce risque prend une dimension particulière lorsque ces dispositifs sont déployés dans des espaces publics, où s'exercent de nombreuses libertés individuelles (droit à la vie privée, liberté d'aller et venir, d'expression et de réunion, droit de manifester, liberté de conscience et d'exercice des cultes, etc.). La préservation de l'anonymat dans l'espace public est une dimension essentielle pour l'exercice de ces libertés ; la captation et, maintenant l'analyse, de l'image des personnes dans ces espaces sont incontestablement porteuses de risques pour les droits et libertés fondamentaux de celles-ci.

Des risques importants pour les libertés individuelles et collectives existent du simple fait de la multiplication, actuelle et anticipée, des dispositifs de vidéo « augmentée » qui pourrait aboutir à un sentiment de surveillance généralisée.

Par ailleurs, la vidéo « augmentée » peut constituer une **technologie invisible et « sans contact » pour les personnes**. Si les citoyens peuvent constater et, d'une certaine manière, appréhender l'installation de différentes caméras vidéo dans leur quotidien, ils n'ont pas de moyen d'avoir conscience que celles-ci peuvent également les analyser, ni de quelle manière et sur quels critères cette analyse fonctionne.

En outre, les technologies de vidéo « augmentée », comme tout traitement algorithmique, présentent un **potentiel d'adaptabilité à des cas d'usage potentiellement illimités** qui doit être pris en compte dans leur perception globale. Ces technologies sont en effet techniquement capables, parfois par de simples réglages, de changer de fonctions : un dispositif de vidéo « augmentée » initialement installé pour réaliser une analyse de la fréquentation d'un lieu (comptage des personnes et segmentation par genre et tranches d'âge) pourrait, assez simplement, permettre le suivi du parcours des personnes. Ou encore, un dispositif de vidéo « augmentée » dans un panneau publicitaire qui affiche de la publicité sur la base de l'âge ou du genre de la personne pourrait techniquement également le faire sur la base de l'analyse de son visage et de ses émotions.

---

[15] Un enregistrement vidéo, quoiqu'il puisse contenir des images révélant des données sensibles ou des données d'infraction, n'est pas considéré en soi comme relevant de ces catégories particulières de données à caractère personnel. En revanche, si les images font l'objet d'un traitement spécifique sur des données sensibles ou d'infraction, l'article 6 de la loi Informatique et Libertés ou 10 du RGPD seraient susceptible de s'appliquer (délibération CNIL n°2020-064)

Dans son rapport sur l'éthique des algorithmes et de l'intelligence artificielle publié le 15 décembre 2017[16], la CNIL pointait la nécessité de garantir les principes de vigilance (visant à se prémunir de la tentation de délégation à ces outils) et de loyauté (afin de s'assurer que l'utilisation des outils correspond à celle attendue), au risque d'observer des dérives pouvant aboutir, comme souligné par le Défenseur des droits, à l'automatisation de discriminations[17]. En effet, le recours aux technologies de vidéo « augmentée » peut, selon des usages, présenter des risques discriminatoires pour les personnes parce que ces technologies peuvent cibler les caractéristiques des individus qui peuvent les exposer à des discriminations (identité de genre, apparence physique, âge, etc.).

Enfin, il convient de considérer que les traitements d'analyse automatique d'images, derrière leur apparente neutralité, sont porteurs de choix normatifs. Ainsi, la façon dont ceux-ci sont formalisés et développés ou les données sur lesquelles ils sont entrainés et évalués conditionnent des choix de fonctionnement, parfois de façon implicite. Ces dispositifs ne sont, par ailleurs, pas exempts d'erreurs et de biais qui pourraient avoir un impact important sur les personnes.

3.2. Des risques gradués en fonction de l'usage des dispositifs

Ces dispositifs, qui offrent un grand nombre d'usages et de fonctionnalités, ne présentent pas tous le même degré d'intrusivité. Cette gradation des risques et de l'impact pour les personnes est fonction de la nature **des informations traitées et des décisions prises à l'issue de l'analyse réalisée par l'outil de vidéo « augmentée »**.

Les dispositifs qui auront pour objectif ou pour effet une prise de décision ou des conséquences au niveau individuel, c'est-à-dire pour une personne en particulier, engendreront une intrusivité et un risque généralement plus élevés pour la personne concernée que ceux qui ne produisent que des informations agrégées ou des décisions concernant un ensemble de personnes. Ce sera par exemple le cas d'un dispositif de vidéo « augmentée » placé dans un panneau publicitaire qui aurait pour objectif d'afficher de la publicité ciblée à une personne en fonction de son genre ou de son âge, ou encore d'un dispositif de vidéo « augmenté » qui aurait pour objectif de détecter des infractions et de faciliter l'appréhension de leur auteur.

À l'inverse, lorsque les dispositifs auront pour seul objet la production d'une information, notamment statistique, pouvant servir à conduire des analyses ou, parfois, aboutir à une décision à portée collective, le niveau d'intrusivité sera moins élevé pour chaque individu composant ce collectif. À titre d'exemple, un dispositif de vidéo « augmentée » déployé dans une station de métro et ayant pour objet d'étudier la densité de fréquentation de la station présentera peu de risques directs pour les personnes présentes si l'objectif du dispositif est seulement de produire un taux de fréquentation, ou d'ajuster et de fluidifier le trafic en temps réel en fonction de l'affluence. Les risques pour les droits et libertés des personnes dépendront du type de décision qui sera prise.

L'impact de ces dispositifs pourra varier en fonction des lieux dans lesquels ils sont déployés et des catégories de population les fréquentant. Ce sera ainsi le cas lorsque ces outils seront installés dans des centres commerciaux ou un magasin de jeux vidéo qui, par nature, seront souvent fréquentés par des mineurs constituant une population vulnérable dont la collecte et le traitement de leurs données à caractère personnel nécessitent une attention particulière. De même ces dispositifs sont déployés dans l'espace public à proximité d'un hôpital, d'un local syndical ou politique ou encore d'un lieu de culte, l'analyse de l'image des personnes fréquentant ces lieux pourrait impliquer le traitement de données sensibles (santé, opinions politiques, appartenance syndicale, religion, etc.).

Ces dispositifs présenteront également de nouveaux enjeux et impacts pour les personnes s'ils ont vocation à entièrement automatiser certaines activités de la vie courante. Cela pourrait par exemple être le cas pour les commerces (magasins dits « autonomes ») qui fonctionneraient uniquement à partir de dispositifs de caméras « augmentées » qui suivraient les clients afin d'analyser leurs achats pour leur permettre de les régler directement (en caisse ou sur une application mobile). Des actes simples et quotidiens, tel que faire ses courses, seraient ainsi filmés et analysés de façon continue engendrant un sentiment de surveillance important, qui deviendrait de plus en plus réel à mesure que ces dispositifs se généraliseraient dans tous les lieux où s'exercent quotidiennement les droits et libertés individuelles (voie publique, transports, commerces, lieux culturels, sportifs, etc.)

[16] « Comment permettre à l'Homme de garder la main ? Rapport sur les enjeux éthiques des algorithmes et de l'intelligence artificielle » sur cnil.fr.

[17] « Algorithmes : prévenir l'automatisation des discrimination » sur defenseurdesdroits.fr.

L'ensemble de ces risques et impacts pour les personnes doit donc être clairement exposé et étudié de manière approfondie et pris en compte dès le développement de ces technologies, suivant le principe de protection des données dès la conception (« *privacy by design* »).

4. Des conditions de licéité différenciées en fonction des objectifs, des conditions de mise en œuvre et des risques des dispositifs de vidéo « augmentée »

4.1. Articulation avec les dispositions du CSI

En l'absence de textes spécifiques encadrant l'usage des dispositifs de vidéo « augmentée », la CNIL a analysé à droit constant les principes applicables à ces dispositifs.

Le code de la sécurité intérieure (CSI) fixe le cadre applicable à la vidéoprotection traditionnelle en encadrant strictement l'implantation des caméras sur la voie publique ou dans les lieux ouverts au public pour des finalités déterminées (protection de bâtiments et de leurs abords, régulation des flux de transport, prévention des atteintes à la sécurité des personnes et des biens, constatation des infractions aux règles de la circulation ou relatives aux dépôts sauvages, le secours aux personnes, etc.).

Aucune disposition du CSI n'encadre, à ce jour, les conditions de mise en œuvre des dispositifs de vidéo « augmentée ».

Pour autant, ces dispositifs de captation et d'analyse automatisée des images (qu'ils soient *ad hoc* ou ajoutés à un système de vidéoprotection préexistant et quelle que soit leur finalité) ne doivent pas être considérés comme étant par principe illicites. En effet, le CSI n'a vocation à régir que les dispositifs relevant de son objet et n'empêche pas le déploiement d'autres dispositifs. En outre, pour les finalités qu'il régit, il n'encadre que la licéité de la captation d'image. Cette analyse a été retenue par la CNIL et le gouvernement s'agissant des dispositifs de détection et de mesure du port de masques dans les transports publics, mis en place sur des caméras de vidéoprotection existantes, à des fins de lutte contre la propagation de l'épidémie de COVID-19[18]. Dès lors, selon la CNIL, le régime de la vidéoprotection prévu par le CSI, y compris ses dispositions pénales (article L.254-1), n'interdit pas toute utilisation de la vidéo « augmentée ».

À l'inverse, du fait de la nature distincte des traitements en cause, la CNIL considère que les caméras encadrées par le CSI ne sont pas *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.

L'analyse de la licéité des traitements algorithmiques sur lesquels repose la vidéo « augmentée » doit donc s'effectuer au cas par cas.

4.2. Les principes communs applicables aux dispositifs de vidéo « augmentée »

Dans la mesure où les dispositifs de vidéo « augmentée » captent et analysent des données, en particulier des images qui permettent d'identifier des personnes, leur utilisation doit **respecter la réglementation applicable en matière de données à caractère personnel (c'est-à-dire le RGPD et la loi Informatique et Libertés).**

Même dans le cas où les images sont anonymisées, voire détruites, très rapidement après leur captation et analyse, ces opérations constituent un traitement de données à caractère personnel si les images contiennent des personnes[19].

[18] La CNIL, à l'instar du ministère de l'intérieur qui les exclut du champ des dispositions relatives à la vidéoprotection, retient une même analyse concernant les webcams procédant, notamment à des fins d'information du public sur les conditions météorologiques, à une transmission directe sur Internet (sans enregistrement) d'images issues d'un lieu ouvert au public, captées dans le cadre d'un plan large et en hauteur excluant manifestement tout risque d'atteinte à la vie privée.

[19] Sur ce point : Ordonnance du Conseil d'État, 18 mai 2020, Surveillance par drones sur conseil-etat.fr ; délibération n° 2015-255 du 16 juillet 2015 refusant la mise en œuvre par la société JCDecaux d'un traitement automatisé de données à caractère personnel ayant pour

En conséquence, 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.

4.2.1. Des finalités déterminées, explicites et légitimes

Les responsables doivent avant tout déploiement de ce type de dispositif avoir clairement défini les finalités poursuivies, qui devront être déterminées, explicites et légitimes (article 5.1.b du RGPD). Le résultat de l'analyse automatisée est à distinguer de l'objectif effectivement poursuivi qui constitue la finalité : ainsi, un dispositif qui analyse et classe la mobilité dans une rue (piétons, vélos, trottinettes, voitures, motos, etc.) n'a pas pour objectif cette classification elle-même mais, par exemple, le réaménagement de la voirie et de l'espace public en fonction des usages.

4.2.2. Une base légale appropriée

La **base légale** permettant de fonder le traitement de données devra être déterminée, au cas par cas, dans les conditions prévues à l'article 6 du RGPD.

Si aucune base légale n'est exclue ou privilégiée par principe, la base légale de « l'intérêt légitime »[20] pourrait ne pas toujours être mobilisable**.**

L'intérêt légitime du responsable de traitement ne peut être retenu que sous réserve de la justification du respect des conditions suivantes :

- légitimité de l'intérêt poursuivi par le responsable de traitement ;
- nécessité du traitement de données envisagé pour répondre à cet intérêt légitime ;
- absence d'atteinte disproportionnée aux intérêts et droits des personnes concernées compte tenu de leurs attentes raisonnables à l'égard de ce traitement.

Certains dispositifs semblent conduire à un déséquilibre manifeste **entre les droits et libertés des personnes et les intérêts du responsable du traitement, notamment en l'absence d'attentes raisonnables des personnes vis-à-vis de l'utilisation de ce type de dispositifs**. Par exemple :

- un dispositif qui conditionne l'appréciation de l'éligibilité à un service public à une analyse algorithmique du comportement des personnes dans l'espace public ;
- un dispositif qui analyse et segmente les personnes sur la base de critères tels que l'âge ou le genre, afin de leur adresser des publicités ciblées (par exemple un panneau publicitaire équipé d'une caméra « augmentée » qui va analyser les personnes passant à proximité pour détecter leur âge et/ou leur genre et leur adresser des publicités ciblées selon ces critères) ;
- un dispositif qui analyse et segmente les personnes sur la base de leurs émotions pour leur proposer des contenus en conséquence : (par exemple un écran équipé d'une caméra « augmentée » qui va analyser l'humeur de la personne afin de lui afficher un contenu adapté).

À défaut de reposer sur une autre base légale, telle que le consentement des personnes, ces dispositifs n'apparaissent pas pouvoir être mis en œuvre. Par ailleurs, certains dispositifs, illicites sur le fondement d'un simple intérêt légitime, pourraient s'inscrire dans le cadre d'une « mission d'intérêt public » : il est alors nécessaire que cette mission soit prévue et encadrée dans le droit de l'Union européenne ou français.

La base légale du « contrat »[21] pourrait être mobilisée pour certains traitements de caméras augmentées à condition, d'une part, qu'un contrat soit conclu entre le responsable et la personne concernée (par exemple un contrat ayant pour objet la fourniture d'un service nécessitant le déploiement des caméras « augmentées ») et, d'autre part, que le traitement automatisé de l'image des personnes par des caméras « augmentées » soit nécessaire à son exécution.

---

finalité de tester une méthodologie d'estimation quantitative des flux piétons sur la dalle de La Défense sur legifrance.fr (demande d'autorisation n° 1833589) position validée par le Conseil d'État, 10ème - 9ème chambres réunies, 08/02/2017, 393714 sur legifrance.fr.

[20] Article 6.1.f) du RGPD

[21] Article 6.1.b) du RGPD

4.2.3. La nécessité et la proportionnalité du dispositif

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.

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 ».

En premier lieu, 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. 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.

En second lieu, conformément au principe de minimisation (article 5.1.c) du RGPD), les données traitées ne devront pas excéder ce qui est **nécessaire** pour atteindre les finalités envisagées.

En troisième lieu, 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. Si cette exigence doit être appliquée en tenant compte de la base légale du traitement, il faut souligner que, même lorsque le traitement est fondé sur le consentement des personnes, qui acceptent ainsi des risques d'atteinte à leur vie privée, la CNIL estime que le traitement est illicite si les risques encourus par les personnes du fait du traitement sont inacceptables au regard des avantages retirés du traitement.

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* »)** doivent être mis en œuvre pour réduire les risques pour les personnes concernées.

À titre d'exemple, certaines garanties peuvent être utilement mises en œuvre concernant la qualité des images (abaissement de la définition, floutage, etc.), le nombre d'images traitées (approche « frugale » en données), le traitement local des données (dans des dispositifs physiquement accolés aux caméras), l'intégration de mécanismes permettant la suppression quasi immédiate des images sources ou la production d'informations anonymes[22] (par exemple pour la réalisation d'opérations de comptage).

Au final, 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.).

4.2.4. La nécessaire information des personnes concernées

[22] Pour être effectif, un processus d'anonymisation doit rendre impossible, en utilisant des « moyens raisonnables », la réidentification des personnes concernées à partir des données produites. Voir à ce sujet les lignes directrices du G29 sur les techniques d'anonymisation sur cnil.fr.

L'ensemble des **droits des personnes** sur leurs données devront être respectés.

Une attention particulière doit être portée à **l'information des personnes,** qui est un élément essentiel pour assurer la loyauté du traitement. Dans le cadre du déploiement de dispositifs de vidéo « augmentée », fournir une information dans des termes clairs et simples conformément au RGPD sera nécessaire, sans être toutefois suffisant.

En effet **cette information devra être adaptée au caractère « sans contact » et novateur de ces technologies**. À ce titre, 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.

4.2.5. Réalisation d'une AIPD et désignation éventuelle d'un DPD/DPO

La mise en œuvre de ces dispositifs nécessitera en principe la réalisation d'une **analyse d'impact relative à la protection des données (AIPD)**[23], en raison du caractère innovant de cette technologie. L'AIPD pourra également être requise si le dispositif procède à une surveillance systématique et à grande échelle. L'AIPD devra être soumise à la consultation obligatoire de la CNIL[24] pour les traitements mis en œuvre par certaines autorités, notamment publiques[25], à des fins de prévention et de détection des infractions pénales.

Enfin, la **désignation d'un délégué à la protection des données (DPD/DPO)** sera obligatoire pour les organismes (utilisateurs ou développeurs de ces solutions) dont les « activités de base » utilisent ces dispositifs « à grande échelle » : cela pourra par exemple être le cas des prestataires ou industriels dont le cœur de métier est le développement de solutions de vidéo « augmentée » et le traitement des données pour le compte de leurs clients, ou encore de centres commerciaux qui procéderaient régulièrement, dans le cadre de leur activité marketing, à la mesure de l'audience de panneaux publicitaires ou à la réalisation d'opérations de prospection ciblée au travers de dispositifs de vidéo « augmentée ».

4.3. La nécessité d'une norme juridique autorisant et encadrant certains des dispositifs

La plupart des dispositifs nécessitent, pour pouvoir être légalement mis en œuvre, l'existence d'un texte de nature législative ou réglementaire les autorisant ou les encadrant.

4.3.1. Nécessité d'une norme au titre de l'article 23 du RGPD

Les dispositifs de vidéo « augmentée » se heurtent généralement en pratique à l'obligation prévue par le RGPD de garantir aux personnes la possibilité de s'opposer au traitement de leurs données.

Selon le RGPD[26] , le droit d'opposition doit être garanti « à tout moment » et effectif.

Or, 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 ce droit. En effet, ces dispositifs captent automatiquement l'image des personnes passant dans leur champ de vision, la traitent souvent instantanément pour en tirer une conséquence en temps réel (calcul d'une donnée, affichage d'une publicité, génération d'une alerte etc.) sans possibilité d'ignorer les personnes qui auraient exprimé préalablement leur opposition ni d'interrompre le traitement. Ainsi, en pratique, les personnes, si elles n'ont pas la possibilité de s'opposer préalablement à l'analyse automatique de leur image, ne peuvent s'opposer au traitement.

En outre, quelle que soit la bonne volonté des organismes, les conditions d'exercice du droit d'opposition apparaissent, la plupart du temps, difficilement acceptables en pratique, indépendamment de leur effectivité, comme par exemples exprimer son opposition par un mouvement corporel significatif, le placement dans un

[23] Article 35 du RGPD sur cnil.fr.

[24] Article 36 du RGPD sur cnil.fr.

[25] Article 90 de la loi Informatique et Libertés sur cnil.fr.

[26] Article 21 du RGPD

espace dédié ou un marquage au sol, le fait de porter un vêtement, emprunter des parcours alternatifs, etc. De telles modalités font souvent peser une contrainte trop lourde - voire irréaliste dans la vie quotidienne - sur les personnes, sont peu praticables dans les faits et difficilement généralisables et impliquent la mise en œuvre d'un traitement de données supplémentaire potentiellement plus intrusif.

Si l'on ne peut exclure que des développements techniques à venir permettent de mettre en place des modalités d'opposition équilibrée, tel n'est généralement pas le cas actuellement.

Par ailleurs, l'existence même d'un droit d'opposition pourrait, dans certains, cas apparaître antinomique avec l'objectif même du traitement : il en va ainsi de la détection de comportements anormaux, suspects ou dangereux à des fins de sécurisation des personnes et des biens.

En conséquence, les dispositifs de vidéo « augmentée » devront, sous réserve de ne pas pouvoir justifier de la mise en œuvre effective et acceptable d'un droit d'opposition ou de pouvoir se prévaloir de l'exception liée à des traitements réalisés à des fins statistiques (voir infra), **être autorisés par un cadre légal spécifique de nature *a minima* réglementaire, conforme aux conditions posées par l'article 23 du RGPD[27].** Un tel acte devra justifier la légitimité et la proportionnalité du traitement opéré au regard de l'objectif poursuivi, la nécessité d'exclure la faculté pour les personnes de s'y opposer, tout en fixant des garanties appropriées au bénéfice de ces dernières.

4.3.2. Nécessité d'une loi au titre de l'article 34 de la Constitution

Certains dispositifs de caméras « augmentées » - tout particulièrement ceux mis en œuvre à des fins de police administrative générale ou de police judiciaire - sont susceptibles d'affecter les garanties fondamentales apportées aux citoyens pour l'exercice des libertés publiques. Dans le prolongement de la jurisprudence du Conseil d'État sur les caméras piétons et les drones[28], la mise en œuvre de tels dispositifs semble relever des domaines constitutionnellement réservés à la loi (article 34 de la Constitution).

Sauf à ce que l'utilisation de tels dispositifs puisse s'inscrire dans les prérogatives de police judiciaire déjà prévues par le code de procédure pénale (pouvoirs généraux d'enquête du procureur de la République et du juge d'instruction)[29], le recours à des analyses algorithmiques d'images de caméras de vidéoprotection, réalisées en temps réel en vue d'une intervention immédiate ou de l'enclenchement de procédures administratives ou judiciaires par les services de police, semble devoir être subordonnée à l'existence d'un encadrement législatif spécifiques. Cette analyse de la CNIL a déjà été relevée dans le rapport « *Pour un usage responsable et acceptable par la société des technologies de sécurité* » remis au Premier ministre par le député Jean-Michel MIS le 20 septembre dernier.

Même en étant temporaires et limités à la protection de certains évènements ou à des finalités de prévention de troubles graves à l'ordre public, ces traitements sont susceptibles de modifier la façon dont l'action des services de police influe sur l'exercice par les citoyens de leurs libertés et droits fondamentaux, et ne peuvent trouver un fondement juridique suffisant dans les dispositions générales de la loi Informatique et Libertés ou dans le pouvoir réglementaire du gouvernement ou, a fortiori, des maires.

Les traitements algorithmiques de détection de comportements « suspects » ou infractionnels emportent un changement de degré et de nature dans la surveillance à distance de la voie publique que le législateur a souhaité encadrer il y a plusieurs années au sein du CSI pour les caméras de vidéoprotection « classiques ». Les nouveaux dispositifs engendrent des risques accrus pour les personnes dépassant la seule problématique de la protection

---

[27] Le considérant 41 du RGPD précise *« Lorsque le présent règlement fait référence à une base juridique ou à une mesure législative, cela ne signifie pas nécessairement que l'adoption d'un acte législatif par un parlement est exigée, sans préjudice des obligations prévues en vertu de l'ordre constitutionnel de l'État membre concerné. »*

[28] 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.

[29] A noter sur ce point qu'une telle analyse n'a pas été retenue par le Conseil d'Etat s'agissant de l'usage de drones lors d'une opération de police judiciaire. En effet, dans son avis rendu public n° 404020 du 12 octobre 2021 (accessible depuis « Consiliaweb »), la Haute juridiction a souligné la nécessité, pour asseoir la légalité d'un tel usage, de l'adoption de dispositions dédiées (en complément des articles 41 et 81 du code de procédure pénale) l'autorisant et l'encadrant spécifiquement.

de leurs données, en touchant à la fois à la sphère pénale (logique répressive) et aux conditions d'exercice de leurs libertés fondamentales (droit à la vie privée, liberté d'aller et venir, de se réunir et de manifester, etc.).

Leur nécessité doit être évaluée à un niveau plus général que les seules collectivités publiques décidant de leur mise en place : l'éventuel déploiement de tels dispositifs intrusifs ne doit pas résulter d'une addition d'initiatives locales, nécessairement sans cohérence. **Seule une loi spécifique, adaptée aux caractéristiques techniques et aux enjeux en cause, pourrait éventuellement, à l'issue d'un débat démocratique, décider de leur légitimité et, par la fixation de garanties minimales, prévoir une conciliation équilibrée entre l'objectif de sauvegarde de l'ordre public et l'impératif de protection des droits et libertés fondamentaux.**

Un rapport d'information sénatorial publié en mai 2022 fait état d'un avis (non publié) par le Conseil d'État qui partagerait cette analyse[30].

En outre, ce rapport du Sénat tend à considérer que la licéité des dispositifs algorithmiques mis en œuvre par les acteurs privés, à des fins de sécurisation des personnes et de biens, devrait également être subordonnée à une intervention spécifique du législateur[31].

Si la répartition entre ce qui relève du domaine de la loi et du règlement ne relève pas de sa compétence, **la CNIL souligne que la nécessité d'une autorisation et d'un encadrement spécifiques de nature *législative* pourrait devoir être étendue à d'autres cas d'usage que ceux ayant spécifiquement trait à la prévention et à la répression des atteintes à l'ordre public par les autorités publiques.**

4.4. Le cas spécifique des dispositifs impliquant des traitements de données à des fins statistiques

Certains dispositifs de vidéo « augmentée » **sont destinés à réaliser des comptages** à des fins « statistiques ». En pratique, ces dispositifs analysent les images issues des caméras afin d'en extraire des informations statistiques, sans que les images soient conservées.

Ces dispositifs, s'ils répondent aux critères d'un traitement de données à des fins statistiques au sens du RGPD et de la loi Informatique et Libertés, bénéficient **d'un régime dérogatoire au titre duquel il est notamment permis d'exclure le droit d'opposition** des personnes[32].

Dans tous les cas, **la CNIL insiste sur le fait que, même s'il ne s'agit que de produire une information agrégée et statistique, le fait de construire cet indicateur par des images filmées dans des lieux publics n'est pas anodin**. De telles « statistiques » ne pourront être réalisées que de manière licite et pour des finalités légitimes. En particulier, tout traitement « statistique », comme tout traitement de données à caractère personnel, devra faire l'objet d'une analyse de licéité, de nécessité et de proportionnalité.

4.4.1. Le champ des traitements de données à des fins statistiques

Pour que ces traitements algorithmiques constituent un traitement de données à des fins statistiques au sens du RGPD, ils doivent répondre aux conditions suivantes :

---

[30] Il s'agit du rapport d'information n° 627 (2021-2022) de MM. Marc-Philippe DAUBRESSE, Arnaud de BELENET et Jérôme DURAIN, fait au nom de la commission des lois, sur la reconnaissance faciale et ses risques au regard de la protection des libertés individuelles. Celui-ci énonce en effet (page 88) que « *selon les informations recueillies par les rapporteurs au cours de leurs auditions, le Conseil d'État aurait, dans un avis rendu le 12 octobre 2021, non publié, estimé que les traitements des images issues de la vidéoprotection par le biais d'un logiciel d'intelligence artificielle constituent des traitements de données personnelles distincts de ceux des images issus de la vidéoprotection et que ceux-ci, compte tenu du changement d'échelle qu'ils impliquent dans la capacité d'exploitation des images de surveillance de la voie publique, sont susceptibles de porter une atteinte telle à la liberté individuelle qu'elle affecterait les garanties fondamentales apportées aux citoyens pour l'exercice des libertés publiques au sens de l'article 34 de la Constitution du 4 octobre 1958. **Le Conseil d'État en déduit qu'une base législative explicite est nécessaire pour encadrer le recours à l'intelligence artificielle sur des images issues de l'espace public, y compris sans utilisation de données biométriques*** ».

[31] En effet, ce rapport (cf. p 89) propose l'adoption d'une base législative « *autorisant, à titre expérimental, les traitements d'images issues des espaces accessibles au public à l'aide de l'intelligence artificielle sans utilisation de données biométriques dans le cadre des finalités attribuées au dispositif de vidéoprotection déployé après autorisation du préfet et consultation, le cas échéant, de la CNIL* ». Il précise que « *cette base législative permettrait ainsi, par exemple : (…) aux acteurs privés de détecter les incidents (incivilités, fraude, délinquance) afin d'améliorer leur gestion des agressions ou des vols dans des lieux et établissements ouverts au public ou dans les abords immédiats de bâtiments et d'installations particulièrement exposés à ces risques* ».

[32] Articles 89 du RGPD éclairé par son considérant 162, articles 78 de la loi Informatique et Libertés et 116 de son décret d'application (décret n° 2019-536 du 29 mai 2019).

- **Le traitement n'a une finalité statistique que s'il tend à la production de données agrégées pour elles-mêmes : le traitement doit avoir pour unique objet le calcul des données, leur affichage ou publication, leur éventuel partage ou communication**. Ces statistiques peuvent ensuite constituer le fondement de décisions ultérieures, individuelles ou collectives, mais le traitement de données à caractère personnel ne vise qu'à la production de la donnée agrégée. Lorsqu'à l'inverse le traitement tend par lui-même à une prise de décision immédiate (déclencher une alerte, afficher une publicité, bloquer l'accès à un quai de gare etc.), sur la base de la donnée ainsi calculée, cette prise de décision fait partie des finalités du traitement, qui ne peut généralement pas être regardé comme uniquement statistique.

- Les résultats statistiques obtenus à partir du traitement des images doivent constituer **des données agrégées et anonymes** au sens de la réglementation sur la protection des données.

À titre d'**illustrations**, peut être considéré comme « statistique » un dispositif permettant de calculer l'affluence dans un métro pour afficher aux voyageurs les rames les moins remplies vers lesquelles se diriger à condition que les résultats soient anonymes ; de même serait statistique le traitement permettant d'analyser le type de fréquentation d'un centre commercial sur la base de critères (genre des personnes et tranche d'âge par exemple) pour permettre au gérant de choisir ensuite les publicités les plus adaptées ; de même pour un dispositif permettant de comptabiliser les flux de visiteurs pour calculer le tarif d'un bail commercial assis sur la fréquentation. Ce traitement, réalisé à partir de l'analyse des images issues des caméras dans le centre commercial, transmet uniquement des informations statistiques sur la fréquentation - par exemple les taux d'hommes et de femmes et ou de personnes ayant entre 25 et 35 ans.

Tous ces traitements seront considérés comme réalisés à des fins de calcul statistique : **les décisions ultérieures sont prises sur le fondement des données anonymes, et non directement à partir des données à caractère personnel des individus qui ont été filmés.**

Au contraire, un traitement modifiant en temps réel les publicités affichés dans un centre commercial en fonction de l'analyse de certaines caractéristiques du public ne pourrait bénéficier du régime des fins statistiques : **la finalité de l'utilisation des données à caractère personnel ne serait alors pas limitée à la production d'indicateurs mais tendrait à l'affichage direct de ces publicités.**

Dans tous les cas, les traitements à finalité statistique doivent respecter l'exigence de conception « privacy by design », en application de l'article 25 du RGPD. Il en résulte notamment que les données les statistiques produites doivent être anonymisées, et les images « source » effacées **le plus rapidement possible**.

4.4.2. L'exclusion possible du droit d'opposition

Les traitements algorithmiques issus d'un dispositif de vidéo « augmentée » qui entrent dans le champ des traitements à des fins statistiques devront répondre aux conditions d'exclusion du droit d'opposition qui sont fixées par :

- l'article 21.6 du RGPD pour les traitements nécessaires à l'exécution d'une mission d'intérêt public ;

- à défaut par l'article 116 du décret du 29 mai 2019 qui permet d'exclure le droit d'opposition[33] dans la mesure où son exercice risquerait « *de rendre impossible ou d'entraver sérieusement la réalisation des finalités spécifiques et où de telles dérogations sont nécessaires pour atteindre ces finalités* ».

En pratique, dans cette dernière hypothèse, le droit d'opposition pourra être exclu :

- si l'exercice de celui-ci empêche l'obtention de résultats statistiques fiables (les résultats statistiques seraient faussés ou inutilisables du fait de l'exercice de ce droit par une partie des personnes concernées) ;

- si aucune modalité effective d'opposition ne peut en pratique être mise en œuvre, ce qui conduirait finalement à renoncer à la production des statistiques et donc à compromettre la réalisation de la finalité du traitement. Il en va de même si les modalités d'opposition techniquement envisageables se révélaient plus intrusives que le traitement de données lui-même.

[33] Dispositions de l'article 78 de loi « informatique et libertés » et de l'article 116 de son décret d'application (décret n° 2019-536 du 29 mai 2019).

Conclusion

Par ce document, la CNIL souhaite préciser, après avoir été sollicitée à de nombreuses reprises, le régime juridique actuel applicable aux caméras « augmentées ». Les conditions d'application à cette nouvelle technologie des règles relatives à la protection des données, et des principes protégeant les droits fondamentaux, sont, en partie, incertaines ou à construire. La CNIL, en prenant position après une consultation publique, a voulu contribuer au débat et sécuriser les acteurs. Elle tiendra évidemment compte de toute évolution des textes ou de la jurisprudence en la matière.

Comme elle l'a souligné, cette technologie ne constitue pas le prolongement des dispositifs existants mais un changement de nature. La CNIL en tire deux conséquences.

D'une part, l'édiction d'un cadre juridique spécifique est souhaitable et nécessitera probablement, de façon générale ou sectorielle, une intervention du législateur. Qu'il s'agisse d'usages qu'il n'appartient qu'au Parlement d'autoriser, ou du besoin d'écarter le droit d'opposition pour autoriser en pratique certains cas d'usage, cette analyse juridique rejoint la nécessité politique, pour la puissance publique, de tracer la ligne, au-delà du « techniquement faisable », entre ce qu'il est possible de faire - parce que socialement et éthiquement acceptable - et ce qui ne l'est pas. C'est un choix autant éthique et politique que juridique.

D'autre part, cette technologie est porteuse d'opportunités mais aussi, à moyen terme, et y compris dans les cas où son utilisation peut être légale et légitime, de risques nouveaux pour certains droits individuels, notamment le droit à la vie privée. Ces risques tiennent à certains usages qui peuvent en être faits mais aussi à l'accumulation d'usages en eux-mêmes admissibles.

La CNIL recommande ainsi au regard de la nature intrusive des dispositifs de caméras « augmentées », que les dispositifs les moins impactants pour les droits et libertés des personnes soient privilégiés lorsque cela est possible. Au surplus, le déploiement de dispositifs de caméras « augmentées » ne pourra se faire sur la seule justification de considérations économiques et devra faire l'objet d'une évaluation rigoureuse de leurs performances techniques et opérationnelles.

En outre, la CNIL appelle avec insistance à une réflexion globale sur le juste emploi des caméras augmentées dans l'espace public afin que soit évitée leur multiplication désordonnée, aboutissant à une densité d'observation automatisée qui modifierait notre rapport à l'espace public – et ce, quelle que soit la légitimité de chaque dispositif pris isolément.

Il reviendra au Parlement et au gouvernement, éclairés par un débat public, de faire des choix. La CNIL recommande, pour sa part, que les usages de ces technologies soient le plus possible localisés et réservés aux cas où ils présentent la plus-value la plus forte, si possible en lien avec l'intérêt général, en les assortissant de garanties appropriées.