PROJET DE POSITION

RELATIVE AUX CONDITIONS DE DÉPLOIEMENT DES CAMÉRAS DITES « INTELLIGENTES » OU « AUGMENTÉES » DANS LES ESPACES PUBLICS

Projet soumis à consultation publique.

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

1. Observations préalables

1.1. 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 couplés à des caméras, permettent d'extraire diverses informations à partir des 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…) ou encore permettant l'identification 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.

1.2. 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 « intelligentes » 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 d'intelligence artificielle**.

1.3. Si le terme « vidéo augmentée » recouvre une grande variété de solutions, **le présent document n'a vocation qu'à traiter des dispositifs, fixes ou mobiles, déployés dans les espaces publics[1] à l'exclusion des dispositifs de reconnaissance biométrique[2]**, 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[3]. Il ne sera pas non plus traité ici des usages de ces dispositifs dans des lieux non ouverts au public (par exemple bureaux, réserves ou entrepôts de magasins…), dans un cadre strictement privé ou encore à des fins de recherche scientifique au sens du RGPD.

1.4. De nombreuses publications en la matière (articles de presse, de recherches, brochures commerciales, guide 2020 de l'association nationale de la vidéoprotection…), 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[4], ou encore le contrat stratégique 2020-2022 de la Filière « industries de sécurité » du Comité national de l'industrie[5].

1.5. 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 et 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.

1.6. **Si les enjeux pour les acteurs, ainsi que la légitimité de certains usages, ne peuvent être ignorés, ils doivent impérativement être considérés au travers du prisme, essentiel dans toute société démocratique, de la protection des droits et libertés fondamentaux des personnes filmées et analysées par ces dispositifs, et en particulier de la protection de leurs données personnelles.**

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

---

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

[2] 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.

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

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

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

1.8. 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[6] 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[7], Conseil de l'Europe[8] et Haut-Commissariat des Nations unies aux droits de l'homme[9]).

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

1.10. 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[10], dont certains ne pouvaient respecter le droit d'opposition prévu par le RGPD.

1.11. **Face à l'absence d'encadrement spécifique de ces dispositifs, la CNIL souhaite aujourd'hui exposer 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).

1.12. **Compte tenu de l'ensemble des enjeux attachés au déploiement de ces dispositifs, la CNIL estime nécessaire que l'ensemble des parties prenantes ait l'opportunité de s'exprimer et de faire valoir ses besoins, ses analyses et ses alertes en la matière.**

1.13. **Elle a donc décidé de soumettre à consultation publique ses réflexions et analyses**. Une telle démarche manifeste sa volonté de mobiliser l'ensemble des acteurs de la vidéo « augmentée » autour des enjeux de protection des droits et libertés fondamentaux et de permettre à tous (citoyens, administrés, consommateurs, industriels/fournisseurs de solutions, utilisateurs de solutions, chercheurs, universitaires, associations…) de lui faire part de leur positionnement vis-à-vis de cette technologie pour déterminer notamment les usages souhaitables, l'encadrement juridique nécessaire et les architectures techniques à promouvoir, notamment en adoptant une approche de protection des données dès la conception (« *privacy by design* »).

1.14. **En d'autres mots, et dès lors que la légitimité de certains usages de ces technologies aura pu être actée, la CNIL estime indispensable d'établir un socle de confiance nécessaire à leur implantation et à leur pérennisation. Un cadre juridique clair 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.**

---

[6] 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.

[7] 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…) 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

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

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

[10] « 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

2.1.1. Le terme retenu par la CNIL de vidéo « augmentée » désigne ici des dispositifs vidéo auxquels sont associés des traitements algorithmiques mis en œuvre par des logiciels, permettant une analyse automatique, en temps réel et en continu, des images captées par la caméra. 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…

2.1.2. 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…), 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…) déterminées en amont par les concepteurs et utilisateurs.

2.1.3. En pratique, les algorithmes 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*.

2.1.4. **Même si ces algorithmes 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 et qui ne cessent de se développer en dépit de l'absence d'études fiables quant à leur efficacité[11].**

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

2.2. Des cas d'usages multiples

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

2.2.2. 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…), 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…) pour poursuivre des objectifs divers.

2.2.3. 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 :

[11] 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 cette problématique du manque d'évaluation.

- **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…), 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…) ;
  - la régulation des flux de circulation et l'aménagement de leur territoire par des collectivités, dans une logique à la fois sécuritaire, écologique et économique. Le dispositif permettrait une comptabilisation et une différenciation en temps réel des usages (piétons, camions, vélos, trottinette…) et leurs cheminements dans des zones spécifiques (centres-villes ou périphéries), permettant ainsi notamment d'identifier et de résoudre d'éventuels conflits d'usage (modification de la signalétique, développement à terme – ou ouverture instantanée - sur la chaussée de voies, pistes réservées à certaines catégories d'usagers…), 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 d'individus par les exploitants de transports publics à des fins d'intervention par les services de sécurité compétents ; ou encore la mesure de l'affluence et de la fréquentation des quais du métro ou de la gare, à des fins de diffusion de messages informatifs dynamiques à l'intention des usagers (zones à éviter, espaces à privilégier…) 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, des salles de concert ou d'autres établissements recevant du public, grâce à la détection de certaines situations ou comportements (port d'objets dangereux, attitudes laissant craindre un vol à l'étalage ou la réalisation d'actes de violence…) ;
  - 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…) ;
  - 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… par exemple :
    - réorganisation du contenu des rayons en considération des typologies de clients et de leurs déplacements au sein du magasin ;
    - ajustement des moyens en personnel / nettoyage de façon dynamique ou en fonction des jours / créneaux horaires les plus fréquentés ;
    - analyse et facturation des achats de manière automatisée (magasins dits « autonomes » sans personnel) ;
    - appréciation de l'utilité d'un *showroom* physique et de la pertinence des produits exposés ;
    - modulation des prix de ceux-ci en fonction des modes d'interaction avec les têtes de gondole / comportements d'achat, ou encore du montant des loyers à payer par les enseignes selon l'emplacement du local, mis en perspective avec les parcours clients, au sein du centre commercial, etc.

2.2.4. **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 sont ainsi censés valoriser des parcs de caméras déjà installés.

2.2.5. **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…) ;
- leur conservation peut être faite 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).

2.2.6. **Il convient également de souligner que ces technologies peuvent être utilisées sans traitement de données personnelles** (par exemple, un système d'analyse de pièces de monnaie sur un tapis roulant).

2.2.7. **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 en particulier des risques qu'ils comportent pour les intéressés.**

2.2.8. L'essor de l'usage de la vidéo pour ces usages s'explique à la fois par les niveaux de performance atteints ces dernières années, une certaine nécessité à justifier les coûts d'installation et de maintenance élevés de réseaux de vidéoprotection existants, la « versatilité » de cette technologie (un capteur vidéo peut être utilisé pour différents usages) et un coût d'exploitation réduit par rapport aux dispositifs vidéo classiques (l'automatisation permettant d'économiser les coûts salariaux des opérateurs de vidéosurveillance), notamment quand les caméras sont déjà implantées dans l'espace public.

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

2.3.1. 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…), ces espaces étant eux-mêmes en extension avec l'essor de la vidéoprotection.

2.3.2. **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[12], **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.

2.3.3. 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 »), les usages de défense, le domaine dit des « villes connectées » ou « *smart cities* » (surveillance de voie publique et infrastructures y compris les usages de mobilité), le commerce de détail (comptage, lutte contre le vol, surveillance des parkings…). Les enjeux en matière de données personnelles se concentrent

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

principalement sur les deux derniers segments. Le marché des caméras « augmentées » pour les usages des particuliers (sécurité et domotique), moins développé et rémunérateur, relève d'un segment différent (et non visé par ce document).

2.3.4. **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 américains, 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.

2.3.5. 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.

2.3.6. Pour certains observateurs, un premier enjeu pour l'économie française est l'emploi. Le secteur de la vidéoprotection emploie 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. Si l'attention est souvent appelée sur des cas d'usage entièrement nouveaux, la principale motivation du déploiement des dispositifs de vidéo « augmentée », si l'on en croit le guide Pixel 2022 de l'AN2V, est le gain en termes de coût permis par la réduction de ces effectifs, avec pour contrepartie un accroissement de l'efficacité opérationnelle.

2.3.7. 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 » ou « *smart cities* ». C'est plutôt cette partie logicielle de la chaîne de valeur de la vidéo « augmentée » 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, 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.

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

3.1.1. Comme évoqué précédemment, **dans un système de caméra vidéo classique, l'image des personnes est visionnée (ou enregistrée) par un nombre limité de personnes habilitées situées derrière un écran de contrôle.** Ces caméras se limitent à capter et à enregistrer les images pouvant être saisies par leur spectre de balayage. En outre, ces images brutes, qui seront en principe 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.

3.1.2. La CNIL considère, dans cette configuration, que seules sont traitées les images de personnes, sans considération pour chacune des informations « en sommeil » y figurant, y compris celles qui permettraient de révéler des informations à caractère sensible (état de santé d'une personne se déplaçant à l'aide d'un chien et d'une canne d'aveugle ou orientation sexuelle d'un couple de personnes s'enlaçant sur la voie publique…), dès lors que ces informations ne font pas l'objet d'un traitement automatisé particulier par le dispositif, pour un usage spécifiquement prédéfini[13].

[13] « Lignes directrices du CEPD 3/2019 sur le traitement des données à caractère personnel par les dispositifs vidéo » (PDF, 358 ko) sur edpb.europa.eu.

3.1.3. L'intégration d'algorithmes dans ces systèmes vidéo, analysant de manière systématique et automatisée les images issues des caméras, a pour conséquence d'élargir considérablement la quantité d'images traitées et des informations qui peuvent en être inférées. **Ces nouveaux outils vidéo peuvent ainsi conduire à un traitement massif de données personnelles, parfois même de données sensibles**.

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

3.1.5. **Un tel changement ne constitue pas une simple évolution technologique ou un approfondissement des dispositifs de vidéoprotection, mais une modification de leur nature.** La CNIL rappelle à cet égard qu'une vigilance particulière doit être accordée vis-à-vis de la tentation du « solutionnisme technologique » qui consisterait ici à considérer que les dispositifs de vidéo « augmentée » sont nécessairement efficaces et permettraient de résoudre par eux-mêmes de nombreux problèmes d'ordre économique ou social.

3.1.6. Pour réguler l'essor de la vidéoprotection, la CNIL a depuis longtemps pointé le risque d'une surveillance généralisée des individus, induit par ces dispositifs. Cette surveillance était cependant, en partie, limitée matériellement par les capacités humaines de visionnage des images. Or, ce risque prend une nouvelle ampleur du fait qu'il se double désormais d'un **risque d'analyse généralisée des personnes** : les dispositifs automatisés offrant un champ, une systématisation et une précision d'analyse impossible 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, du fait de leur importante capacité d'analyse, offrent 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…).

3.1.7. Ce risque d'analyse généralisée prend une dimension particulière lorsque ces dispositifs sont déployés dans des espaces publics, où s'exercent par nature 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…). 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.

3.1.8. Au-delà des risques que présente chaque traitement de données, induit par le déploiement de dispositifs de vidéo « augmentée » pris isolément, **des risques importants pour les libertés individuelles existent du simple fait de leur généralisation (actuelle et anticipée) qui pourrait aboutir à un sentiment de surveillance généralisée.**

3.1.9. 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, non pas seulement les filmer, mais également les analyser.

3.1.10. En outre, les technologies de vidéo « augmentée », comme tout traitement algorithmique, présentent un **potentiel de versatilité** 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 également le suivi du parcours des personnes au sein de ce lieu. Ou encore, un dispositif de vidéo « augmentée » dans un panneau publicitaire qui adresse 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.

3.1.11. Enfin, comme pour tout traitement automatisé, il convient de bien considérer que les algorithmes 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. Comme pointé par la CNIL dans son rapport sur l'éthique des

algorithmes et de l'intelligence artificielle[14], il convient donc 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 sinon d'observer des dérives pouvant par exemple aboutir, comme souligné par le Défenseur des droits, à l'automatisation de discriminations[15].

3.1.12. **Ces dispositifs, qui offrent un grand nombre d'usages et de fonctionnalités, ne présentent pas tous le même degré d'intrusivité.**

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

3.2.1. Cette gradation des risques et de l'impact pour les personnes est fonction de la nature **des informations et décisions prises à l'issue de l'analyse réalisée par l'outil de vidéo « augmentée »**.

3.2.2. **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 nécessairement 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 » dans un panneau publicitaire qui aurait pour objectif d'adresser 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 son auteur.

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

3.2.4. Dans tous les cas, la CNIL insiste sur le fait que ces dispositifs présentent une intrusivité particulière : 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. C'est pourquoi un encadrement spécifique est souhaitable.

3.2.5. L'**impact de ces dispositifs, même lorsqu'ils ne visent qu'un collectif de personnes, pourra varier en fonction des lieux dans lesquels ils sont déployés et ainsi 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 personnelles nécessitent une attention particulière ; ou encore si ces dispositifs sont déployés dans l'espace public à proximité d'un hôpital ou d'un lieu de culte, l'analyse de l'image des personnes fréquentant ces lieux pourrait impliquer le traitement de données sensibles (santé, religion, etc.).

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

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

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

4. Des conditions de légalité 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

4.1.1. **En l'absence de textes spécifiques encadrant l'usage des dispositifs de vidéo « augmentée », la CNIL a analysé à droit constant les principes communs applicables à tous dispositifs et les conditions spécifiques de déploiement de certains.**

4.1.2. **À titre liminaire**, il convient de rappeler que 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 déterminés (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…).

4.1.3. **Aucune disposition du CSI ne vient spécifiquement encadrer les conditions de mise en œuvre des dispositifs de vidéo « augmentée ».**

4.1.4. Pour autant, on ne peut déduire de cette absence que les traitements de captation et d'analyse automatisée des images, mis en œuvre au moyen de ces dispositifs (qu'ils soient *ad hoc* ou par l'ajout à un système de vidéoprotection préexistant) doivent être considérés comme étant par principe illicites car non prévus par le CSI. En effet, celui-ci n'ayant vocation à régir que les dispositifs relevant de son objet, il n'a pas d'effet limitatif sur des projets poursuivant des finalités sans lien direct avec la préservation de l'ordre et de la sécurité publics. Une telle analyse a ainsi été récemment 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 à des fins de lutte contre la propagation de l'épidémie de COVID-19[16]. Dès lors, selon la CNIL, le régime de la vidéoprotection prévu par le CSI, y compris ses dispositions pénales, n'interdit pas, par lui-même, toute utilisation de la vidéo « augmentée ».

4.1.5. **Les traitements algorithmiques sur lesquels repose la vidéo « augmentée » relèvent dès lors, comme tout traitement de données à caractère personnel, du cadre général de la réglementation applicable en matière de protection des données à caractère personnel** (RGPD, loi Informatique et Libertés) qui s'impose à l'ensemble des opérations sur des données se rapportant à des personnes physiques identifiées ou potentiellement identifiables.

4.1.6. À l'inverse, la CNIL considère que les caméras encadrées par le CSI ne sont pas non plus *de facto* « autorisées » à utiliser des technologies de vidéo « augmentée » pour les finalités ayant permis leur implantation : le législateur n'a clairement entendu régir et autoriser que des dispositifs de vidéo « simples », qui ne captent pas le son et ne sont pas équipés d'algorithmes d'analyse automatique.

4.2. Les principes communs applicables à tous les dispositifs de vidéo « augmentée »

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

[16] 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.

4.2.2. Il faut rappeler que, 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[17].

4.2.3. En conséquence, les utilisateurs de ces solutions (acteurs publics ou privés), et leurs concepteurs (sociétés qui développent et commercialisent les dispositifs de vidéo « augmentée ») 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.

4.2.4. Des finalités déterminées, explicites et légitimes

4.2.4.1. À ce titre, ils devront avant tout déploiement de ce type de dispositif, même à titre expérimental, avoir clairement défini les finalités poursuivies, qui devront être déterminées, explicites et légitimes (article 5.1.b du RGPD). Il est important de ne pas retenir le résultat de l'analyse automatisée dans la détermination de la finalité en omettant l'objectif opérationnel effectivement poursuivi. 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.

4.2.5. Une base légale appropriée

4.2.5.1. La ou les **bases légales appropriées** permettant de fonder les traitements de données impliqués devront également être déterminées, au cas par cas, dans les conditions prévues à l'article 6 du RGPD.

4.2.5.2. La CNIL a pu relever au cours de ses travaux, que si aucune base légale n'est exclue ou privilégiée par principe, **certains dispositifs ne pourront en principe pas se fonder sur l'intérêt légitime car leur configuration et les traitements de données qu'ils impliquent ne permettraient pas d'assurer une juste balance entre les droits et libertés des personnes et les intérêts du responsable du traitement, notamment en l'absence d'attentes raisonnables des personnes à l'égard des traitements de données impliqués.**

4.2.5.3. La CNIL estime ainsi que ne pourraient en principe pas reposer sur l'intérêt légitime :

- des dispositifs qui analysent et segmentent les personnes, sur la base de critères tels que l'âge ou le genre afin de leur adresser des publicités ciblées ;
- des dispositifs qui analysent et segmentent les personnes sur la base de leurs émotions ou de données sensibles (santé, religion, orientation sexuelle, etc.) ;
- des dispositifs qui analysent le comportement et les émotions des personnes sur la base de la détection de leurs gestes et expressions, ou de leurs interactions avec un objet ;

4.2.5.4. A défaut de reposer sur une autre base légale, telle que le consentement des personnes, ces dispositifs n'apparaissent pas pouvoir être légalement mis en œuvre.

4.2.6. La nécessité et la proportionnalité du dispositif

4.2.6.1. En fonction de la base légale retenue, le responsable du traitement devra justifier de la **nécessité d'utiliser des systèmes de vidéo « augmentée »**, notamment par l'évaluation de l'existence ou non de moyens moins intrusifs permettant d'atteindre les finalités envisagées (par exemple : capteurs infrarouges, enquêtes de fréquentation ou d'usage, vigiles, effectifs de police, capteurs de véhicules sur la chaussée, détecteur de présence, capteurs de dispositifs électroniques utilisant les technologies Bluetooth ou Wi-Fi…) et l'évaluation de l'utilité, de la performance opérationnelle du dispositif au regard de l'objectif poursuivi (évaluation qui doit considérer le dispositif dans son environnement et non de façon isolée).

4.2.6.2. Par ailleurs, en fonction des bases juridiques retenues, le responsable de traitement devra s'assurer que l'atteinte à la vie privée demeure **proportionnée** au regard des intérêts, droits et libertés des

[17] 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 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.

personnes concernées, notamment grâce aux garanties qu'ils présentent. À ce titre, la CNIL considère que l'intégration de **mécanismes effectifs de protection de la vie privée dès la conception (« *privacy by design* »)** doivent être mis en œuvre. À titre d'exemple, différentes modalités concernant, la qualité des images (abaissement de la définition, floutage…), le nombre d'images traitées (approches frugales en données), le temps de traitement des images ou encore le traitement local des données (dans des dispositifs physiquement accolés aux caméras) peuvent permettre de réduire considérablement les risques pour les personnes concernées et contribuer à respecter le principe de proportionnalité et de minimisation des données.

4.2.6.3. À ce titre, l'intégration de mécanismes de traitements automatisés permettant à la fois la suppression quasi-immédiate des images sources et la production d'informations anonymes (par exemple pour la réalisation d'opérations de comptage), peut également apporter des garanties fortes. La CNIL rappelle toutefois que pour être effectif, un processus d'anonymisation doit rendre impossible l'identification des personnes concernées à partir des données produites[18].

4.2.7. Le respect des droits des personnes concernées

4.2.7.1. Les **droits des personnes** sur leurs données personnelles devront évidemment être respectés.

4.2.7.2. À ce titre, une attention particulière doit être portée à **l'information des personnes.** La transparence est en effet un élément essentiel pour assurer la loyauté du traitement. Toutefois, dans le cadre du déploiement de dispositif de vidéo « augmentée » fournir une information dans des termes clairs et simples conformément aux articles 12 à 14 du RGPD sera nécessaire et essentiel sans être suffisant pour assurer le respect du principe de transparence.

4.2.7.3. La CNIL considère en effet que **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 traditionnels d'un système de vidéoprotection, tels qu'on peut aujourd'hui les trouver dans les lieux publics, ne saurait à priori assurer pleinement la bonne et complète information des personnes concernées. Il sera donc essentiel de porter à la connaissance des personnes concernées l'information clé du dispositif qui réside dans le caractère « augmenté » des caméras et les finalités qu'ils poursuivent. La fourniture de cette information sur des supports adaptés (panneau d'information, vidéos, codes QR, information sur le site, marquages au sol, annonces sonores…) est encouragée pour assurer une information claire.

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

4.2.8.1. La mise en œuvre de ces dispositifs nécessitera en principe la réalisation d'une **analyse d'impact relative à la protection des données (AIPD)**[19], notamment au regard du caractère innovant et de la surveillance systématique et à grande échelle qu'engendrent ces technologies. Cette AIPD devra par ailleurs être soumise à la consultation obligatoire de la CNIL[20] pour les traitements qui seraient mis en œuvre par une autorité compétente[21] et à des fins de prévention et de détection des infractions pénales.

4.2.8.2. Enfin, la **désignation d'un délégué à la protection des données (DPD/DPO)** pourra également s'avérer obligatoire pour les organismes (utilisateurs ou développeurs de ces solutions) dont les « activités de base » consistent notamment en l'utilisation de 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 solution 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 ».

---

[18] Voir à ce sujet les lignes directrices du G29 sur les techniques d'anonymisation sur cnil.fr.

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

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

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

4.3. La nécessité d'une norme autorisant et encadrant la plupart des types de dispositifs

4.3.1. **À l'occasion de l'examen des différents cas d'usage portés à sa connaissance, la CNIL a estimé que la plupart des dispositifs nécessitaient, pour pouvoir être légalement mis en œuvre, l'existence ou l'intervention d'un texte de nature législative ou réglementaire les autorisant et les encadrant.**

4.3.2. **D'une part, la CNIL considère que les dispositifs de vidéo « augmentée » se heurtent généralement en pratique à l'obligation prévue par le RGPD de garantir aux personnes concernées la possibilité de s'opposer au traitement de leurs données.**

4.3.3. Le droit d'opposition doit en effet être garanti « à tout moment » par le responsable du traitement lorsque celui-ci se fonde sur un intérêt public ou son intérêt légitime[22]. Or, la mise en œuvre des dispositifs de vidéo « augmentée » dans l'espace public ou ouverts au public apparait se heurter, dans la pratique, à l'obligation de prendre en compte et de respecter de manière effective ce droit d'opposition. En effet, les dispositifs vidéo captent automatiquement l'image des personnes passant dans leur spectre de balayage et la traitent souvent instantanément, sans possibilité d'éviter les personnes ayant exprimé préalablement leur opposition ou d'interrompre le traitement. En pratique, ces personnes pourront uniquement obtenir la suppression de leurs données, lorsqu'elles auront été conservées, et non éviter leur traitement.

4.3.4. La CNIL a pu constater que quelle que soit la bonne volonté des organismes à cet égard, les conditions d'exercice du droit d'opposition apparaissent la plupart du temps, difficilement acceptables en pratique, indépendamment de leur effectivité. Les modalités d'exercice envisageables font souvent peser une contrainte trop lourde, voire irréaliste, sur les personnes (restriction importante de leurs possibilités de circulation, obligation d'adopter une gestuelle particulière ou de porter un signe distinctif stigmatisant…) De plus, certaines modalités d'exercice du droit d'opposition impliquent la mise en œuvre d'un traitement de données supplémentaire potentiellement plus intrusif (prise en considération de l'apparence vestimentaire des individus pour qu'ils soient reconnus lors de leur passage devant la caméra et automatiquement exclus du dispositif d'analyse des flux de fréquentation). Si l'on ne peut exclure que des développements techniques à venir permettent de mettre en place des modalités d'opposition équilibrée, la CNIL estime que tel n'est pas le cas actuellement.

4.3.5. Par ailleurs, l'existence même d'un droit d'opposition pourrait, dans certains, cas apparaître antinomique avec l'objectif poursuivi par le traitement : il en va ainsi de toutes les fois où il s'agit, pour des gestionnaires de lieux ouverts au public, de détecter des comportements anormaux, suspects ou dangereux à des fins de sécurisation des personnes et des biens.

4.3.6. **En conséquence, pour la CNIL, 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 (cf. infra), être autorisés par un cadre légal spécifique de nature *a minima* réglementaire, conformément à l'article 23 du RGPD.** Un tel acte devra acter 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.

4.3.7. **Cette analyse juridique rejoint la nécessité, 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 qu'il ne l'est pas. C'est un choix autant juridique, éthique que politique.**

4.3.8. **D'autre part, il semble que, dans le prolongement de la jurisprudence du Conseil d'État[23], certains de ces dispositifs, et tout particulièrement ceux mis en œuvre à des**

---

[22] Article 21 du RGPD

[23] 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

fins de police administrative ou judiciaire – donc de prévention ou de répression d'atteintes à l'ordre public -, soient susceptibles d'affecter les garanties fondamentales apportées aux citoyens pour l'exercice des libertés publiques. La mise en œuvre de tels dispositifs relève à ce titre des domaines constitutionnellement réservés à la loi (article 34 de la Constitution).

4.3.9. La CNIL considère que la légalité du 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, est subordonnée à l'existence d'une autorisation et d'un encadrement législatifs 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.

4.3.10. À cet égard, même en étant limités à la protection de certains évènements ou à des finalités de prévention de troubles graves à l'ordre public, ce type de traitements - même temporaires - sont susceptibles de modifier par principe et tellement profondément, la façon dont l'action des services de police influe sur l'exercice par les citoyens de leurs libertés et droits fondamentaux, qu'ils ne peuvent dès lors trouver un fondement juridique suffisant dans les dispositions générales de la loi Informatique et Libertés ou dans le seul pouvoir réglementaire du gouvernement ou, à fortiori, des maires.

4.3.11. Les algorithmes de détection de comportements « suspects » ou infractionnels, au profit de services publics bénéficiant de prérogatives de puissance publique particulières (et notamment de pouvoirs de contrainte et d'engagement de poursuites), emportent un changement de degré et de nature dans la surveillance à distance de la voie publique que le législateur a encadrée pour les caméras « simples ». Ces dispositifs engendrent des risques accrus pour les personnes dépassant la seule problématique de la protection 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.).

4.3.12. Leur 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 : l'éventuel déploiement de tels dispositifs intrusifs ne doit pas résulter d'une addition d'initiatives, nécessairement sans cohérence. Pour la CNIL, **seule une loi spécifique, adaptée aux caractéristiques techniques et aux enjeux en cause, pourrait, 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.**

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

4.4.1. Dans le cadre de ses travaux, la CNIL a pu constater qu'un certain nombre de dispositifs de vidéo « augmentée » **sont destinés à réaliser des comptages** conduisant à des analyses « statistiques » au sens du RGPD. En pratique, ces dispositifs analysent très rapidement les images issues des caméras afin d'en extraire des informations, qualifiées de statistiques, qui sont ensuite traitées sans que l'image ne soit conservée.

4.4.2. La CNIL a donc étudié si de tels dispositifs pouvaient répondre aux critères d'un traitement de données à des fins statistiques au sens du RGPD et de la loi Informatique et Libertés permettant **l'application d'un régime dérogatoire au titre duquel il est notamment permis d'exclure, le cas échéant, le droit d'opposition** des personnes concernées[24].

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

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.

[24] 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).

4.4.3.1. Pour que ces traitements algorithmiques constituent un traitement de données à des fins statistiques, la CNIL considère qu'ils devront répondre aux conditions cumulatives suivantes :

- En premier lieu, les résultats statistiques obtenus à partir du traitement de données ne doivent pas constituer des données à caractère personnel mais **des données agrégées et anonymes** au sens de la réglementation sur la protection des données.

- En second lieu, le traitement n'a une finalité statistique que s'il tend à la production de ces données agrégées pour elles-mêmes, afin de permettre éventuellement leur utilisation dans un second temps. Le fait, pour un dispositif qui se fonde sur une donnée agrégée, d'avoir une portée opérationnelle, pour permettre une réaction concrète en temps réel, lui fait généralement perdre sa qualification de « statistique » et donc le bénéfice du régime dérogatoire afférent. En principe, la CNIL considère qu'il doit exister un **délai entre la captation des données par le dispositif permettant la production des résultats statistiques et leur exploitation par le responsable du traitement**.

4.4.3.2. Ceci joue de telle façon que, en cas d'utilisation de caméras augmentées pour calculer des statistiques sur un flux de personnes, l'éventuelle mesure prise par le responsable de traitement s'applique à un groupe de personnes nécessairement différent du groupe sur lequel porte l'information (la « statistique »). En outre, ainsi que le rappelle le considérant 162 du RGPD, les résultats statistiques ne sont en principe pas utilisés en tant que tels à l'appui d'une décision ou mesure concernant une personne physique en particulier.

4.4.3.3. À titre d'**illustrations**, la CNIL considère comme statistique un dispositif permettant d'analyser le type de fréquentation d'un centre commercial sur la base de critères tels que le genre des personnes et leur tranche d'âge pour afficher ultérieurement des publicités adaptées à la fréquentation du lieu ou de comptabiliser les flux de visiteurs pour calculer les baux commerciaux (assis sur la fréquentation) des différents exploitants. Ce traitement, 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. Ce traitement sera considéré comme réalisé à des fins statistiques si les publicités affichées sur la base de ces résultats statistiques ne sont pas déterminées immédiatement, mais par exploitation ultérieure des données statistiques. Par exemple, les publicités pourraient être adaptées, si l'utilisation de la vidéo augmentée est jugée nécessaire et proportionné dans ce contexte, chaque week-end en fonction de l'analyse des résultats statistiques des week-ends précédents.

4.4.3.4. Au contraire, un tel traitement ne serait pas réalisé à des fins statistiques si les publicités étaient modifiées en temps réel en fonction de la fréquentation du lieu : sa finalité ne serait pas la production d'indicateurs mais directement l'affichage de ces publicités.

4.4.3.5. Lors des échanges qu'elle a eus avec les professionnels, la CNIL a pu constater qu'un certain nombre d'usages ayant des finalités de sécurité civile, ou sanitaire, ou de fluidification du trafic et présentant des atteintes faibles pour les personnes, ne sont pas autorisés par la réglementation actuelle, lorsqu'ils ne constituent pas des traitements statistiques, faute de pouvoir en pratique respecter le droit d'opposition. En l'état de sa réflexion, la CNIL estime donc qu'il revient aux pouvoirs publics de décider s'ils autorisent ces traitements, qui impliquent que les personnes soient filmées et analysées sans pouvoir s'y opposer. De même, si les traitements statistiques semblent plus aisément conciliables avec le cadre juridique actuel, la CNIL appelle à ce que l'usage de statistiques automatiquement générées par des caméras dans des espaces ouverts au public soit spécifiquement défini et réglementé, eu égard à leur nature particulière.

4.4.4. Les conditions d'exclusion du droit d'opposition

4.4.4.1. Les traitements algorithmiques impliqués par un dispositif de vidéo « augmentée » qui entrent dans le champ des traitements à des fins statistiques devront également répondre aux conditions d'exclusion du droit d'opposition qui sont fixées par l'article 116 du décret n° 2019-536 du 29 mai 2019.

4.4.4.2. En vertu de ce texte, le droit d'opposition peut être exclu[25] 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* ».

4.4.4.3. En pratique, la CNIL considère que cela signifie que 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.

[25] 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).