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

Réponse AN2V
à la consultation lancée par la CNIL

SOMMAIRE

1. Introduction

1.1. Rappel du contexte

La CNIL a publié un projet de position relative aux conditions de déploiement des caméras dites intelligentes dans les espaces publics. Elle constate en effet une tendance visant à la multiplication de dispositifs constitués de logiciels de traitements automatisés couplés à des caméras, qui permettent d'extraire diverses informations à partir des flux vidéo qui en sont issus.

Elle a ainsi 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 personnelles dès la conception (« privacy by design »).

1.2. An2v, une association reconnue dans le domaine de la vidéoprotection – vidéosurveillance

L'association nationale de la vidéoprotection a été fondée en 2004. Elle est née d'un besoin de mutualisation des connaissances dans ce domaine. Elle vise ainsi à identifier et encourager les bonnes pratiques et les technologies utiles à la sécurité des biens et des personnes.

Elle associe depuis son origine trois publics :

- **Utilisateurs publics et privés** de technologies de sûreté : villes, centres commerciaux, banques, sites sensibles…
- **Institutionnels** concernés par cette thématique : ministères, forces de sécurité intérieure…
- **Fournisseurs** de technologies de sûreté : bureaux d'études, constructeurs, intégrateurs…

L'AN2V est très représentative des entreprises fournissant des solutions de sûreté. En, effet, en décembre 2021, elle compte 155 membres, pour la plupart des constructeurs et grands intégrateurs. **Elle regroupe quasiment tous les constructeurs de logiciels d'analyse d'image**.

A ce titre, **notre association est directement concernée par la consultation publique lancée par la CN**IL sur les caméras augmentées.

1.3. Quel est le but de cette contribution ?

Conformément à la philosophie qui anime nos travaux, nous souhaitons que le cadre juridique de la vidéosurveillance et de la vidéoprotection permette de tirer le meilleur parti possible des technologies au service de la sécurité, **en prenant en compte la nécessaire protection des libertés publiques**.

Notre démarche s'inscrit dans une **volonté d'ouverture et de proposition constructive**. Ce document vise à réaliser une synthèse des remarques effectuées par nos membres durant des réunions distancielles. Nos entreprises ont besoin de **visibilité** pour leurs activités. Elles ont besoin de pouvoir **expérimenter**, afin de savoir répondre aux demandes des opérateurs et de maintenir une **souveraineté** dans le domaine de l'intelligence artificielle appliquée aux caméras. Elles se heurtent quotidiennement à des difficultés d'ordre juridique et souhaitent une **clarification de la réglementation de la vidéosurveillance-vidéoprotection**, ce qui va bien au-delà d'un ajustement législatif prenant en compte l'analyse d'image.

1.4. Comment et par qui cette contribution a-t-elle été élaborée ?

La CNIL a porté à notre connaissance la mise en œuvre de cette consultation. Nous avons aussitôt mobilisé nos entreprises membres en organisant un groupe de travail permettant de recueillir leurs contributions.

Nous n'avons pas opté pour un commentaire point par point du projet de position de la CNIL. Nous proposons plutôt une présentation structurée par thème des attentes de nos membres.

2. Les attentes prioritaires des entreprises membres de l'AN2V

Se concentrant sur leur métier, celui d'apporter des solutions aux entités qui assurent la sécurité des citoyens et des biens, et plus généralement contribuent au respect de la loi, une préoccupation du citoyen qui va de pair avec la protection de sa vie privée, les entreprises membres de l'AN2V ont analysé le projet de position et ont exprimé des attentes qui ne relèvent pas uniquement de la réglementation. Elles ont relevé **le rôle important joué par l'humain** et particulièrement les agents qui utilisent les dispositifs de vidéoprotection - vidéosurveillance, en insistant sur la nécessité de **formations adaptées**. Elles revendiquent **un droit à l'expérimentation** et, sur ce terrain pas totalement défriché, souhaitent une **meilleure collaboration avec les institutions concernées**, dont la CNIL.

2.1. L'humain au cœur du dispositif

2.1.1. Ne pas opposer les hommes, qui gardent le dernier mot, et les technologies

On oppose souvent les hommes et les technologies. Les technologies de sécurité avancées basées sur l'IA sont, aujourd'hui et à moyen terme, avant tout un outil d'aide à la décision. Elles ne viennent pas remplacer l'Humain, d'ailleurs difficile à recruter, mais visent à l'aider dans ses tâches quotidiennes. La finalité des caméras concernées n'est pas sensiblement altérée. De fait, la consultation de la CNIL porte au moins autant sur la notion « d'opérateur vidéo augmenté », que de « caméra augmentée ».

Le développement de la vidéoprotection - vidéosurveillance conduit à ce que des sites recensent plusieurs centaines de caméras, avec un nombre constant d'opérateurs en charge de leur exploitation. Le recours à des dispositifs avancés de gestion des images en temps réel et en temps différé est indispensable à l'efficacité des dispositifs.

Certains considèrent que la vidéoprotection est inefficace, mais refusent les solutions permettant de l'optimiser. Pourtant, on ne peut pas à la fois reprocher aux systèmes de ne pas être efficaces, et refuser les solutions qui facilitent le travail des opérateurs, en temps réel ou en relecture.

- **En temps réel :**

Nombre d'algorithmes de vision par ordinateur offrent un palliatif à ce manque de ressources et permettent d'attirer l'attention d'un humain sur les scènes présentant un intérêt. Cela présente de nombreux avantages. Préempter l'affichage de l'opérateur sur les vues pertinentes par le biais d'une analyse d'images permet ainsi de consacrer moins d'attention à d'autres vues, et diminue ainsi le risque de biais de l'opérateur ou de tentations pour lui de suivre tel ou tel phénomène, voire le risque qu'il surveille à titre personnel, ou au profit d'un tiers, des lieux ou des gens qu'il connaît. On peut faire une analogie avec la télésurveillance. La caméra augmentée devient un capteur qui envoie des alertes à l'opérateur, lequel réalise une levée de doute. Nous considérons que ce fonctionnement est bien moins attentatoire aux libertés individuelles qu'une surveillance aléatoire.

- **En temps différé :**

Des solutions permettent de faciliter les relectures et simplifient le travail des enquêteurs. Il faut prendre conscience que dans beaucoup de dispositifs, il n'y a pas d'opérateur H24, et ce sont les OPJ qui doivent parfois visionner des heures d'images sans indexation des événements. Des solutions de recherche par critères permettent de gagner des heures de travail pour des enquêteurs.

2.1.2. Améliorer la formation des agents en charge de l'exploitation et de l'encadrement

La formation à ces nouvelles technologies et aux nouveaux modes de fonctionnement qui en découlent est un levier à favoriser. Elle est indispensable compte-tenu de l'évolution des technologies. Nous observons que l'élément humain possède un rôle déterminant sur les conditions d'exploitation des systèmes.

L'IA ne présume pas : seul le regard et l'interprétation humaine conduisent à une action ou à une procédure.

Nous pensons qu'une formation des opérateurs, basée sur les « bons usages » est préférable à des interdictions. L'encadrement de ces agents est également fondamental. Tous ces logiciels devront être paramétrés. Les personnels en charge de cette mission doivent être formés.

Une forme d'assermentation / habilitation des opérateurs mettant en œuvre des caméras augmentée est évoquée par le groupe de travail, un peu sur le modèle de la vidéoverbalisation.

2.1.3. Faire monter le niveau de compétence et les responsabilités de l'écosystème

Plus généralement, la particularité assez unique du présent exercice est qu'il se situe dans un contexte triplement émergeant : qu'il s'agisse des matières scientifiques et techniques, des bonnes pratiques juridiques et administratives relatives à la protection des données personnelles, ou de l'organisation des entreprises et autres entités pour prendre en compte les problèmes posés, les formations académiques commencent tout juste à se saisir du domaine, le référentiel normatif est en cours d'élaboration, etc. Seuls quelques très gros opérateurs disposent aujourd'hui d'une expertise, reconnue et confiante en ses positions.

Dans ce contexte, les acteurs de l'AN2V sont convaincus qu'il faut aider et encourager les différents acteurs à faire éclore un écosystème vertueux performant, utilisant les mécanismes définis dans le RGPD ; ils souhaitent que se construise un consensus de toutes les parties vers un mode de fonctionnement où, à terme, ce seraient les acteurs du terrain eux-mêmes qui réguleraient la mise en œuvre des « caméras augmentées », la CNIL n'étant saisie qu'en cas de questionnement des acteurs, de dérive ou d'infraction.

2.2. Faciliter les expérimentations et apprentissages légitimes

2.2.1. Des enjeux de souveraineté

Garder des compétences en France dans le domaine de la vidéo augmentée par l'IA est un enjeu économique, **un enjeu de souveraineté**. Pour cela, l'expérimentation est indispensable. Nos membres concernés par ce sujet souhaitent la mise en place d'un droit (encadré) à l'expérimentation à grande échelle dans les lieux ouverts au public. Ils doivent pouvoir rester compétitifs par rapport à leurs concurrents étrangers, soumis à des réglementations différentes (y compris en Europe…). Les grands opérateurs français, eux-mêmes grands exportateurs, ont besoin de rester à la pointe des bonnes pratiques en matière de sécurité.

Pour un acteur industriel, il n'est pas concevable de « brider » l'innovation sous couvert qu'il existerait déjà une ou plusieurs technologies qui remplissent tout ou partie de la fonction demandée. Faire mieux ou différemment, fait partie des objectifs que tout acteur industriel vise afin de renforcer son attractivité sur le marché.

Cette consultation doit participer à favoriser l'émergence de leaders français de la vidéoprotection - vidéosurveillance et ne doit pas aboutir à des **règles qui pourraient entraver leurs développements à la faveur d'acteurs non souverains**.

Si aucun dispositif de ce type ne peut être déployé tant qu'un décret ou une loi n'est pas publié, les acteurs du domaine ne pourront se développer et risqueront de disparaître. Et lorsque qu'un texte sera enfin passé (ce qui risque de prendre beaucoup de temps dans le contexte d'élections présidentielle et législatives qui est le nôtre) ne resteront que des acteurs étrangers pour répondre à la demande.

2.2.2. Propositions pour favoriser l'expérimentation

Les membres du groupe de travail ont émis plusieurs propositions visant à favoriser l'expérimentation encadrée de ces nouvelles technologies :

- La **mise en place d'une procédure allégée**, applicable à un périmètre clairement encadré, associant les propriétaires des caméras et les entités (si elles sont différentes) souhaitant mener des expérimentations en conditions réelles et en présence du public.
- Le texte de la CNIL est muet sur la collecte des informations sur les jeux d'apprentissage pour entrainer les IA. On pourrait **s'appuyer sur le DPO du site concerné**, qui s'engage sur l'apprentissage, la durée des données...
- La **mise à disposition de datasets ciblés**, par la CNIL ou toute autre autorité compétente, permettrait la détection de biais pour ainsi garantir les principes de vigilance, de loyauté et éviter toutes formes de discrimination.
- Créer un **groupe de travail** en vue d'aboutir à une certification commune permettrait de garantir la bienveillance des logiciels d'intelligence artificielle.
- Il faudrait admettre, mais combattre (pour la réduire au maximum) la problématique du **biais de l'apprentissage**.
- Il faudrait enfin **évaluer** les expérimentations mises en place.

2.3. Un souhait de collaboration avec la CNIL

On l'aura compris à la lecture de ce qui précède, les entreprises membres de l'AN2V ont insisté sur leur souhait de mettre en place une **collaboration étroite avec la CNIL**. Elles souhaitent travailler de manière pragmatique et constructive pour faire avancer les technologies au bénéfice de la sécurité publique, dans le respect des libertés individuelles. Elles refusent une approche dogmatique basée sur l'interdiction pure et simple de toute évolution technologique.

Une clarification des missions, du rôle de la CNIL

L'organisation, les missions, les textes portés par la CNIL sont méconnus des professionnels du secteur. Nous pensons qu'une communication ciblée aux acteurs du secteur des technologies de sûreté est à prévoir. AN2V se tient à la disposition de la CNIL pour mettre en place des liens avec ses entreprises membres.

Pédagogie et communication

Le site Internet de la CNIL est une bonne base de connaissance qui mériterait d'être développée. La CNIL a produit des fiches pratiques sur certains sujets (vidéosurveillance au travail, à l'école) que nous relayons régulièrement auprès de nos entreprises. Nous souhaiterions que cela puisse être développé sur plus de sujets, dont l'IA et les technologies telles que la détection sonore, la LAPI…

Une CNIL plus à l'écoute des professionnels

Nos entreprises souhaitent avoir des échanges réguliers avec les instances juridiques concernées pour maintenir le dialogue et aborder les évolutions technologiques à venir.

Elles soulignent le délai de réponse à leurs demandes par mail. Elles regrettent de ne pas avoir de « guichet unique », d'interlocuteur dédié, de mail direct.

Elles évoquent fréquemment la période durant laquelle la CNIL avait engagé un travail avec AN2V, concernant la lecture automatisée de plaques. Elles souhaiteraient pouvoir mettre en place de nouveaux groupes de travail de ce type à l'avenir.

Il est suggéré que le responsable du traitement puisse justifier de la nécessité d'utiliser des systèmes de vidéo "augmentée" à partir de critères mis à disposition par la CNIL, ou toute autre autorité compétente, permettant de déterminer et évaluer précisément le besoin amenant à utilisation de la vidéo augmentée plutôt qu'un autre moyen potentiellement moins intrusif.

De manière générale, ce qui est exprimé est un souhait d'ouverture de la CNIL, en particulier en matière d'évolutions technologiques, un esprit de collaboration et de transparence avec les acteurs concernés.

Rôle du DPO ?

En ligne avec la perspective de professionnalisation évoquée en 2.1.3 de cette note, le groupe de travail a eu de nombreuses discussions sur le DPO, qui est devenu l'interlocuteur principal dans les projets de vidéoprotection - vidéosurveillance avancés.

Ce qui est soulignée fréquemment, c'est le manque de compétences et/ou de craintes des DPO dans le domaine de la sûreté. Dans le doute, par manque de connaissances techniques, le DPO risque de bloquer un projet. Il y a sans doute des formations à imaginer dans ce domaine. Cela étant, nos entreprises soulignent que l'opacité de la réglementation ne facilite pas le travail des DPO.

Un DPO a pour rôle de faire respecter un cadre juridique. Dans ce contexte, ce n'est pas à lui de prendre des décisions structurantes sur le bien-fondé de l'utilisation de tels dispositifs et d'en porter l'entière responsabilité. De nombreux projets ou expérimentation n'aboutissent pas car le DPO refuse d'en prendre la responsabilité, car il ne peut pas s'appuyer sur un cadre. La loi doit donc être suffisamment précise/claire (notamment sur les cas d'usage) pour permettre au DPO de prendre ses décisions sereinement. Il convient donc de définir le cadre, les cas d'usage et les conditions qui permettent d'utiliser ce type de technologie.

2.4. Attentes concernant la réglementation

La réglementation a vocation à formaliser et solidifier l'ensemble des pratiques associées à l'usage des caméras augmentées, dans le contexte général de la sécurité intérieure. Elle est constituée de nombreuses strates. Sa refonte, en cohérence avec les textes européens, nécessitera un travail long et complexe.

L'AN2V est disposée à accompagner cet effort, et souhaite que des dispositions transitoires soient mises en place pour que les difficultés relevées dans la présente contribution puissent être gérées rapidement dans l'intérêt de tous.

2.4.1. Constat

Le cadre juridique de la vidéoprotection - vidéosurveillance est mal connu des professionnels concernés : installateurs, utilisateurs… À leur décharge, on ne peut que constater la grande complexité de notre cadre juridique. Dans ce contexte, utilisateurs et fournisseurs sont souvent désorientés. Même les juristes professionnels ont des analyses contradictoires sur les textes. « *Nul n'est censé ignorer la Loi* » : encore faut-il que celle-ci soit claire et compréhensible par tous. Voici les principales difficultés qui ont été mises en avant par nos membres :

A. Une coexistence de nombreux textes

- Le code de la sécurité intérieure (CSI) : il dispose d'un titre dédié à la vidéoprotection mais regroupe également dans d'autres parties des dispositions relatives à d'autres types de dispositifs : caméras piétons, caméras embarquées dans des véhicules ou des aéronefs.
- La réglementation sur les données à caractère personnel : loi de 1978, RGPD, Directive Police-Justice.
- Le code du travail.
- Le code civil.
- Le code pénal.
- Des textes spécifiques à certaines activités (casinos, stades, transports de fonds).
- Le code général des collectivités territoriales.

B. De multiples critères à prendre en compte

La mise en œuvre de ces textes varie selon des critères de lieu (voie publique, lieu ouvert au public), des critères liés à la nature du dispositif (CSI - Article L251-1) ou à la qualité des personnes mettant en œuvre ces technologies (autorité publique, employeur, commerçant…).

C. Des interprétations différentes des textes

Cette réglementation fait parfois l'objet d'interprétations différentes, y compris au plus haut niveau.

Les préfectures n'ont par exemple pas toutes la même doctrine concernant la mise en œuvre du CSI (durée de conservation des images différente pour des sites et des finalités similaires par exemple).

Les institutions concernées peinent à s'accorder sur les règles à appliquer : la CNIL apporte des informations parfois contradictoires avec celles données par le ministère de l'Intérieur (et réciproquement). Nous soulignons l'effort de pédagogie réalisé par la CNIL dans le domaine de la vidéoprotection – vidéosurveillance, notamment au travers des fiches pratiques mises en ligne sur son site Internet. Toutefois, certaines informations sont inexactes. Par exemple, concernant les lieux d'habitation, la fiche indique que les parties communes des habitations sont des lieux ouverts au public si on y accède sans badge ou code d'accès. De fait, l'installation de caméras dans ces espaces relèverait d'une autorisation préalable du préfet. Or, cette affirmation est contredite par une jurisprudence constante.

De plus, la CNIL change parfois de doctrine, elle a ainsi longtemps admis que les attributs (couleur de vêtement par exemple) n'étaient pas des données à caractère personnel, et revient aujourd'hui sur cette position.

Enfin, la CNIL ne prend jamais de position écrite sauf lorsqu'elle prend une délibération, ce qui laisse souvent les personnes qui la consultent dans l'embarras.

En synthèse, ce contexte n'aide pas les professionnels, qui ne sont pas tous des juristes, à être irréprochables dans la mise en œuvre de cette réglementation. Ils doivent pouvoir s'appuyer sur des informations claires et fiables fournies par les institutions concernées.

D. Une réglementation sur les données à caractère personnel difficile à appliquer

Les textes relatifs à la protection des données n'évoquent pas spécifiquement les dispositifs technologiques de sûreté. On parle de manière générique de traitements de données. De fait, il est parfois difficile pour les professionnels de comprendre les modalités concrètes de mise en œuvre de cette réglementation. Les DPO ne sont pas toujours force de conseil dans ce domaine, faute de compétences spécifiques dans ce domaine très technique.

En outre, il semblerait que les interprétations dans l'ensemble des États soumis à cette réglementation sur le traitement de données à caractère personnel, peuvent parfois différer.

La réglementation porte précisément sur le traitement des données à caractère personnel, et non sur la donnée elle-même. Il serait important de préciser à partir de quel seuil on entre dans ce type de traitement : Repérer un chien errant ou un départ de feu est-il un traitement de donnée à caractère personnel ? Détecter une foule soudaine est-il un traitement de données à caractère personnel ?

E. Une coexistence de lieux de nature différente sur le même site

L'exemple le plus parlant est celui d'un centre commercial, situé à proximité d'une voie publique, et disposant à la fois d'espaces publics et privés, avec du personnel travaillant dans des espaces filmés. Coexistent ainsi des dispositifs de vidéoprotection, et de vidéosurveillance, avec plusieurs réglementations différentes.

Qui plus est, la nature des lieux sur un même site peut varier selon les périodes : ouverture / fermeture d'un lieu ouvert au public.

F. Des contradictions entre le CSI et la réglementation sur les données à caractère personnel

Les dispositions du CSI relatives aux dispositifs de vidéoprotection ne prennent pas en compte la réglementation sur la protection des données. On peut par exemple citer le cas des panneaux d'information du public, dont le contenu fixé par le CSI n'est pas conforme aux préconisations de la CNIL.

Comme la CNIL le souligne dans son projet, le CSI ne prend pas non plus en compte les évolutions technologiques majeures enregistrées ces dernières années, notamment dans le domaine de l'analyse d'images. Le dernier arrêté fixant les normes techniques en vidéoprotection date de 2007.

Pour autant, **la question est de définir à quel moment une technologie s'écarte du droit en vigueur**. Dans sa proposition, la CNIL part du principe que tout est traitement de données à caractère personnel, ce que nous contestons. Nous considérons qu'à très court terme, un rafraîchissement mesuré des dispositions du CSI relatives aux dispositifs vidéo, introduisant une certaine capacité de traitement et la possibilité de réaliser les apprentissages correspondants, permettrait de résoudre rapidement les principales difficultés, lorsque la finalité des dispositifs est la sécurité du citoyen et des infrastructures. Il faut noter à ce sujet que l'European Data Protection Board (EDPB) a adopté début 2020 un référentiel d'application du RGPD aux dispositifs vidéo (Guidelines 3/2019 on processing of personal data through video devices), qui évoque les « caméras augmentées », sans avoir besoin d'introduire, pour les appréhender, de procédures particulières. Ces recommandations sont plus souples que le cadre proposé par la CNIL dans son projet de position.

Toutefois, le souhait de nos membres est une **remise à plat générale de la réglementation actuelle**, avec l'élaboration d'un texte général unique dédié à tous les dispositifs vidéo, prenant en compte le droit européen sur la protection des données à caractère personnel. Nous avons toutefois conscience que certains espaces, comme les établissements scolaires, sont particulièrement sensibles et doivent sans doute bénéficier d'un statut dérogatoire.

G. Une interdiction de principe

Il semble ressortir du projet de la CNIL que « ce qui n'est pas autorisé est interdit ». Nos membres craignent que sous couvert du principe de droit à l'image, de droit à l'opposition, toute forme de technologie avancée dans le domaine de la vidéoprotection soit prohibée.

Le constat est qu'il est difficile de définir un usage ou un domaine d'application de manière univoque. De fait, on peut distinguer trois cas de figure :

- Une zone blanche : ce qui est autorisé
- Une zone noire : ce qui est interdit
- Une zone grise, qui, suivant la position de la CNIL et du législateur, va être autorisée ou interdite

Dans cette zone grise :

- Si ce qui n'est pas autorisé est interdit : la zone grise est assimilée à la zone noire
- Si ce qui n'est pas interdit est autorisé : la zone grise est assimilée à la zone blanche

Entre les deux, il y a certainement moyen de qualifier un peu mieux ce qui mériterait d'être blanc (conditionnel et non présent) et ce qui nécessite « décidemment » d'être noir.

Nous suggérons que le texte de la CNIL précise, dans l'attente d'un texte réglementaire ou législatif spécifique, **les contours de ces différentes « zones ».**

Plus largement, nos membres estiment qu'il ne doit pas y avoir d'interdiction générale basée sur des considérations idéologiques. Une interdiction éventuelle doit relever du législateur.

H. Un grand flou dans la mise en œuvre des technologies

Nos installateurs - intégrateurs sont totalement désorientés face aux demandes de leurs clients qui souhaitent mettre en œuvre des technologies avancées telles que l'analyse d'image, la lecture automatique de plaques d'immatriculation (LAPI), la visualisation de plaques d'immatriculation (VPI), la lecture de plaques d'immatriculation (LPI), la détection de signatures sonores… Ces demandes ne relèvent pas d'une addiction à la technologie mais

correspondent à des besoins fonctionnels, auxquelles de nouvelles solutions peuvent répondre utilement, et pas uniquement dans le domaine de la sûreté. L'AN2V a mis en place en 2021 un **groupe de travail visant à recenser les usages possibles d'une caméra**. Plus de 180 applications ont ainsi été recensées, notamment dans le domaine de l'environnement, de la gestion urbaine. Il appartient maintenant au législateur de décider quels usages justifient le recours à ces nouvelles technologies.

Par ailleurs, les caméras et les algorithmes d'analyse vidéo sont utilisés non seulement pour des usages liés à la sécurité, mais de plus en plus pour extraire des informations « métier » des images, comme par exemple la mesure de fréquentation d'un site.

Il n'existe pas de texte spécifique. La mise en œuvre relève de l'interprétation. Certains utilisateurs refusent de mettre en œuvre ces technologies par peur d'être sanctionnés (ou "avertis défavorablement et publiquement" ce qui revient au même) ! D'autres les installent et les utilisent. Une même demande va obtenir des réponses différentes selon les commissions départementales de vidéoprotection. Il est regrettable que la commission nationale de vidéoprotection (CNV) soit devenue muette sur toutes ces divergences et inexistante sur sa mission initiale.

En résumé, la profession est désorientée. Peu de ressources sont disponibles sur les sites institutionnels, même si là encore nous soulignons l'effort fait en ce domaine par la CNIL.

2.4.2. Les propositions des entreprises membres de l'AN2V

Le constat étant posé, nos entreprises ont proposé des pistes pour résoudre ces difficultés. Elles sont dans une approche constructive, et espèrent que leurs demandes pourront être prises en compte.

A. Une remise à plat de notre réglementation

Nous avons évoqué plus haut le souhait d'obtenir des solutions à court terme par un aménagement des textes du CSI. Cela étant, nous insistons sur la nécessité d'une totale redéfinition de notre réglementation concernant les dispositifs de prise d'image à des fins de sécurité - sûreté.

- **Un texte unique dédié à la captation des images par des caméras dites de surveillance ou de protection**

Notre attente principale est une simplification de la réglementation par l'élaboration d'un texte législatif unique dédié aux caméras, qu'elles soient fixes ou mobiles, installées dans un lieu public ou privé ouvert au public, ou privé, intelligentes ou basiques.

- **Donner un cadre juridique clair à certaines technologies de sûreté spécifiques**

Nous attendons de nos institutions qu'elles donnent un cadre juridique clair et spécifique à toutes les technologies utilisées dans la sûreté. On peut notamment citer la **détection d'anormalité sonore** ou la **lecture automatisée de plaques d'immatriculation** qui ne relèvent d'aucun texte spécifique à ce jour. Leur mise en œuvre ne relève pas forcément de la réglementation sur les données à caractère personnel (audio). Il en va de même pour l'utilisation des informations « métier » des images, comme par exemple la mesure de fréquentation d'un site.

- **Donner un cadre juridique aux métadonnées**

Nous attirons l'attention des institutions concernées sur le fait que les caméras ne produisent plus seulement des images, mais également des données. La plupart des caméras du marché intègrent des solutions d'analyse d'images. Les données créées par les caméras (métadonnées) ne sont pas évoquées par la réglementation.

Nous recevons de multiples questions relatives au statut, à la durée de conservation, à l'utilisation de ces métadonnées.

Simplifier les procédures

Quel que soit le cadre juridique donné à la vidéoprotection - vidéosurveillance augmentée, nos membres souhaitent qu'il soit basé sur la simplicité. Il ne s'agit donc pas d'ajouter des procédures de demandes d'autorisation ou des déclarations supplémentaires à celles pouvant déjà exister.

Nous souhaitons ainsi des formalités uniques qu'un site soit équipé de vidéosurveillance ou de vidéoprotection, ou des deux. Nous considérons que rien ne justifie de différencier un espace privé d'un espace public. Un espace privé peut accueillir des salariés, des visiteurs, au même titre qu'un espace ouvert au public. Pourquoi un système devrait-il être plus encadré qu'un autre en raison du lieu ? Si la vidéo augmentée présente un risque pour les libertés, elle doit être encadrée de la même manière partout.

Prendre en compte le contexte

- **Un site peut changer de nature en fonction des horaires**

Un vaste sous-ensemble de l'espace public devient privé à certaines heures ou certains jours (fermeture). Il conviendrait de définir que ce changement de statut s'accompagne également d'une levée des limites posées à l'analyse d'images.

- **Des événements particuliers peuvent justifier une analyse**

On pourrait imaginer que des événements graves puissent justifier la mise en œuvre de solutions d'analyse avancées : enlèvement, disparition inquiétante, individus dangereux recherchés…

3. Remarques de nos membres sur certaines propositions de la CNIL

Au-delà de la position de l'AN2V synthétisée ci-dessus, ses membres participant aux travaux ont souhaité réagir à différentes dispositions figurant dans le projet de position de la CNIL ; ces remarques et questions figurent ci-après à toutes fins utiles.

3.1. Une approche trop large de la caméra augmentée

3.1.1. Une notion de données à caractère personnel trop imprécise

Le groupe de travail souhaite que soit précisé ce que l'on entend par donnée à caractère personnel. Plusieurs cas concrets ont été relevés lors des réunions de notre groupe de travail :

- La couleur d'un véhicule ou d'un vêtement est-elle une donnée à caractère personnel ?
- Est-ce que l'on traite réellement des données à caractère personnel lorsque les technologies rendent anonymes certaines informations ? Par exemple l'agrégation de données sur les applications statistiques.
- Les « informations en sommeil ». Lors de la captation des données, si seul le squelette de la personne concernée est traité, laissant ainsi de nombreuses informations captées non analysées. Peut-on considérer ces informations comme étant « en sommeil » et de facto ne faisant pas partie d'un traitement de données à caractère personnel ?
- Une plaque d'immatriculation est-elle une donnée à caractère personnel si on ne peut pas la rapprocher d'un fichier permettant d'identifier son propriétaire ?

Il apparaît ainsi que cette notion a priori simple soulève de multiples questions, qui restent le plus souvent sans réponse, ce qui souligne là encore la nécessité d'une clarification ou de validations de la part de la CNIL.

3.1.2. Un changement d'usage, pas de nature

Au paragraphe 2.1.4 de sa proposition, la CNIL considère que « le traitement de données […] change la nature et la portée de la vidéo […] ». Nous considérons que la nature même de la vidéo n'est pas modifiée puisque les données sont issues d'un flux en temps réel qui reflète une situation exacte et nécessairement à jour, mais change la nature de l'usage qui en est fait.

Au paragraphe 2.2.3 de sa proposition, la CNIL utilise le terme « présumer » or le rôle de l'IA est uniquement « d'alerter » pour mettre en avant une situation relevant potentiellement d'un cas d'infraction. Seul le regard et l'interprétation humaine envisage ou non une action ou une procédure. Les vidéos d'un grand nombre de caméras de vidéosurveillance ne sont aujourd'hui pas visionnées, que ce soit en temps réel ou différé, en raison du coût que cela représente en ressources humaines. Et lorsque des agents sont présents pour visionner les images, ils peuvent être responsables de 50 à 100 caméras en même temps, ce qui limite grandement leur capacité à détecter toutes les situations dignes d'intérêt. Nombre d'algorithmes de vision par ordinateur offrent un palliatif à ce manque de ressources et permettent d'attirer l'attention d'un humain sur les scènes présentant un intérêt (ex. détection de gestes suspects). On est là dans un cas d'aide à la décision.

Il faut donc distinguer l'intelligence artificielle de la machine qui pourrait remplacer celle de l'humain, et l'intelligence humaine qui est un outil d'aide à la décision.

3.1.3. Différents niveaux de traitement à distinguer

Le terme de vidéo augmentée retenu par la CNIL dans sa proposition nous paraît trop large. A notre sens, il convient de distinguer plusieurs niveaux de traitements, dont certains ne semblent pas concernés par ce texte. Une classification a ainsi été proposée par nos membres :

- **C1 : Vidéo augmentée sans discernement de mobiles :**

Traitement vidéo ne disposant d'aucun algorithme permettant de détecter des personnes ou des véhicules : détection de la perte d'image, détection d'une fumée dans le ciel ou en hauteur, mesure du niveau d'eau d'un cours d'eau, surveillance de l'état des infrastructures publiques, ...

A notre sens ces algorithmes ne doivent relever d'aucune autorisation préalable, même si des personnes venaient à passer dans les images au moment où l'algorithme effectue sa détection, pourvu que le traitement ne conserve pas leur image.

- **C2 : Vidéo augmentée avec discernement de mobiles, mais pas de personnes :**

Traitement vidéo ne disposant d'aucun algorithme permettant de détecter des personnes : détection d'animal errant, mesure des traversées d'animaux, ouverture automatique d'une borne sur une rue piétonne sur détection d'un véhicule d'urgence, affichage d'un message ou commande d'un dispositif (feu rouge, borne) sur mesure de vitesse, etc...

- **C3 : Vidéo augmentée dédiée aux infractions routières**

Exemples : contre-sens, circulation sur voie interdite, stationnement ou arrêt interdit, dépôt illégal de gravats/déchets depuis un véhicule, etc.).

A notre sens, ces usages sont assimilables aux contrôles routiers automatisés, et le fait qu'ils soient effectués depuis une caméra ou depuis un appareil dédié contenant une caméra ne devrait pas changer le contexte légal et demander les mêmes précautions (affichage) et permettre les mêmes types de contestations (ANTAI).

- **C4 : Vidéo augmentée avec discernement des personnes, mais sans données personnelles :**

Exemples : comptage, détection d'intrusion, détection de course rapide, détection de débordements de personnes sur la rue ou sur les rails, ou chutes dans l'eau, entrée par la sortie, vérification des limites de jauge définies par les autorités dans des espaces publics dangereux : passerelles, balcons, terrasses, détection de la présence d'une arme, ... On notera que les transporteurs publics demandent aujourd'hui des fonctions de détection de landaus,

d'appareils de mobilité pour personnes handicapées… Nous avons besoin d'un cadre juridique précis sur ces fonctions.

Ces traitements devraient faire l'objet d'une autorisation préalable motivée mais il est reconnu que leur contexte est fréquemment légitime (encadrement "léger" par l'usage et le contexte). La détection d'une personne sortant une arme à feu dans une vue vidéo se justifie par la proportionnalité entre le danger de l'arme (même si c'est un jouet factice), et le faible impact du déclenchement d'un affichage automatique de l'image alertant l'opérateur vidéo. Si cet opérateur ne voit pas l'arme ou n'est pas attentif à l'alerte, l'affichage disparaît sans autre conséquence.

- **C5 : Vidéo augmentée avec discernement des personnes et données personnelles :**

Tout traitement caractérisant une propriété relative à une personne observée, quelle que soit cette propriété : couleur de vêtement ou de peau, sexe, âge, démarche, objets portés, etc.

C'est à notre sens la cible que devrait viser la note de la CNIL.

3.1.4. Propositions de nos membres sur les usages

Proposer une liste de finalités qui préciserait les possibles usages de sécurité civile, sanitaire ou de fluidification du trafic présentant une atteinte faible voire inexistante sur les personnes.

Créer une liste exhaustive d'infractions dont les conséquences sur la personne sont moindres. Les contraventions pourraient donc être une première approche de l'utilisation de la vidéo augmentée dans le cadre de procédures administratives ou judiciaires par les services de police.

Restreindre les déploiements uniquement dans le cas d'usage « profilage » et autoriser les déploiements pour les autres applications sans impact comme la détection des bagages abandonnés, la détection de chutes ou de malaises.

Différencier les usages sûreté des usages sécurité ou l'envoi systématique d'une alerte est primordiale (site SEVESO par exemple).

3.2. Préciser le concept de « floutage »

La CNIL utilise le terme de "floutage", nous souhaiterions davantage de précisions à ce sujet. Qu'en est-il des dispositifs et technologies de pseudonymisation ? Sont-ils réversibles ou pas ? Quel est l'intérêt de leur mise en place ? Quelle est la temporalité (captation/analyse/conservation) de leur effectivité ? Quelles sont les technologies/méthodes à favoriser ?

3.3. Sur le droit d'opposition

Nous considérons que le droit d'opposition n'est pas automatique, et que le responsable de traitement peut en refuser l'exercice s'il démontre qu'il existe des motifs légitimes et impérieux pour le traitement, qui prévalent sur les intérêts et les droits et libertés de la personne concernée.

Par conséquent, pour des traitements dont la finalité est fondée sur un intérêt légitime, comme par exemple, la sécurisation des biens et des personnes, il nous semble que le droit d'opposition n'est pas obligatoire.

Il est souhaité que la CNIL fournisse des exemples de mise en œuvre de droits d'opposition qui sont acceptables en pratique.

Concernant le paragraphe 4.4.4.3, dans le cas où le traitement ne rentre pas dans les exceptions mais que l'impossibilité de maintenir le droit d'opposition est présente, il faut permettre de mesurer au sein de l'AIPD les risques et la pertinence de ne pas garder le droit d'opposition.

3.4. Sur la proportionnalité

Concernant le paragraphe 4.2.6.1 « [...] le responsable du traitement devra justifier de la nécessité d'utiliser des systèmes de vidéo « augmentée ».

Il est souhaité que la CNIL, ou toute autre autorité compétente, mette à disposition un outil et/ou des critères chiffrés permettant de déterminer et évaluer précisément le besoin amenant à l'utilisation de la vidéo augmentée plutôt qu'un autre moyen potentiellement moins intrusif.

3.5. Sur la mise en œuvre des caméras augmentées à des fins statistiques

En premier lieu, il existe des cas d'utilisation d'algorithmes à des fins statistiques pour lesquels le respect d'un délai entre captation et exploitation des données va à l'encontre de la finalité.

Il ne faut pas systématiquement réduire l'utilisation à un strict usage en temps différé. Réduire l'utilisation des données issues des caméras « augmentées » à des traitements différés revient à se priver d'outils précieux dans le cadre des missions de maintien de la sécurité et/ou de la tranquillité. Par exemple, tout en prenant bien en compte l'exigence de ne traiter/agréger que des données anonymes, la capacité à mesurer « en temps réel », un taux de présence ou d'occupation (personnes ou voiture) dans un lieu donné, peut permettre de détecter des situations inhabituelles (à la hausse ou à la baisse) et ainsi de donner un temps d'avance à l'opérateur pour décider, si des actions sont à prendre pour éviter que la situation de ne se dégrade. Charge à lui, dans le cadre d'une procédure établie, de valider si les indicateurs remontés nécessitent cette prise de décision. Il va sans dire que toute situation inhabituelle ne requiert pas nécessairement une intervention humaine. Les indicateurs fournis dans cet exemple ne sont que des « facilitateurs » pour la prise de décision, bien souvent ces indicateurs sont transmis de façon plus aléatoires (détection par hasard par un opérateur ou constat de la situation dégradée c'est-à-dire lorsqu'il est trop tard). On voit bien qu'utiliser ce type d'information a posteriori a un intérêt statistique mais qu'on se prive d'une connaissance disponible en réduisant le contexte d'utilisation.

On notera que dans le cadre d'information a posteriori, l'information « Meta data » se suffit à elle-même (si on considère que le moyen de calcul est fiable). Dans le cadre du temps réel, on souhaite laisser l'humain décider, donc la levée de doute nécessitera un accès au flux vidéo (comme c'est déjà le cas dans un CSU à ce jour) et la « Meta data » seule n'est pas suffisante.

3.6. Sur la notion de versatilité

La CNIL évoque la versatilité des caméras augmentées.

Une application de comptage de personnes est incapable, sauf si on l'en a dotée volontairement, de mesurer les âges des personnes. Ainsi, si le principe de privacy by design est respecté dès la conception et dans les stratégies de développement des entreprises éditrices de logiciel, et que la législation encadre les finalités et l'usage, il n'est pas à craindre des usages cachés ou imprévus.