Observations de la Délégation à la protection des données (DPD) de la Ville et de l'Eurométropole de Strasbourg dans le cadre de la consultation publique portant sur la vidéo dite « augmentée » ou « intelligente »

Table des matières

La Ville et Eurométropole de Strasbourg assurent une gestion de la protection des données à caractère personnel par la Délégation à la protection des données (« DPD » ci-après).

La DPD a souhaité contribuer à la consultation publique lancée par la CNIL au sujet de son projet de position relatif aux conditions de déploiement des caméras dites « intelligentes » ou « augmentées » dans les espaces publics. Sa position se veut en concertation avec les métiers de nos collectivités tels que le Centre de Supervision de la Vidéo (CSV), le Service Information et Régulation Automatique de la Circulation (SIRAC) ou encore les Archives. Ses travaux seront par ailleurs partagés avec le corps électif compétent ainsi que le Comité d'éthique sur la vidéoprotection, instance rattachée à nos collectivités.

Le lectorat du document trouvera une première partie qui regroupe l'ensemble des remarques transverses (avant-propos) puis une deuxième reprenant la structure du projet de prise de position de la CNIL (parties I, II, III).

Avant-propos : observations transversales et complémentaires de la Délégation à la protection des données

Suite à la lecture du projet de position de la CNIL, la DPD a constaté que certaines thématiques n'ont, en l'état, pas été abordées dans ce document. Il apparaît pour autant opportun que les autorités de contrôle européennes se penchent sur ces sujets aux enjeux réels en termes de protection des données.

A. Cycle de vie

1. Gestion des données (garanties d'un risque minimal)

Pourrait-on considérer ces infrastructures comme étant d'importance vitale (par analogie d'OSE/OIV) ?

- **Opérateur de services essentiels (OSE)**

Les opérateurs de services essentiels (OSE) ont été mis en place suite à la directive Network and Information Systems (NIS), texte européen, transposé en droit français.

Les OSE sont désignés parmi les organisations qui supportent des services dits essentiels au fonctionnement de la société ou de l'économie et dont la continuité pourrait être gravement affectée par des incidents touchant les réseaux ainsi que les systèmes d'information nécessaires à la fourniture desdits services.

La directive NIS s'applique également aux fournisseurs de service numérique (FSN) qui doivent dans ce cas justifier de la sécurité de leur système d'information.

Ce sont des personnes morales fournissant notamment une place de marché en ligne, un moteur de recherche en ligne ou encore un service d'informatique en nuage (cloud).

Ainsi, il peut être intéressant qu'une concertation entre l'autorité de contrôle et les ministères concernés débouche sur un avis autour des solutions technologiques applicables à la vidéocaptation comme des services relevant *a minima* du statut d'OSE prévu par la directive NIS.

En outre, il semble nécessaire que les autorités compétentes au niveau étatique se prononcent dans le même temps sur ce point pour une harmonisation législative du fait de la généralisation de cette technologie applicable à la vidéocaptation.

- **Opérateurs d'Importance Vitale (OIV)**

La Loi de Programmation Militaire (LPM) du 18 décembre 2013 définit une entité spécifique portant le nom d'Opérateur d'Importance Vitale (OIV). Cette loi est codifiée dans le Code de la défense. Les collectivités territoriales concernées par ce dispositif sont celles qui se sont vues désignées par arrêté.

Les OIV sont les organisations qui, si elles venaient à subir un incident grave, pourraient porter gravement atteinte au potentiel de guerre ou économique, à la sécurité ou à la capacité de survie de la Nation ou mettre gravement en cause la vie de la population. Il s'agit des secteurs du transport, de l'énergie ou encore les industries de défense.

La LPM édicte l'obligation pour les OIV de protéger leurs systèmes d'information d'importance vitale (SIIV) concourant aux activités d'importance vitale.

Dans le cadre de son projet de position, dans son point 2.3.3, la CNIL indique que le marché de la vidéo « augmentée » se situe autour de 4 usages principaux dont « l'usage de défense » ou encore le domaine dit de « villes connectées » (surveillance de voie publique et infrastructure) ».

Pour cette raison, à l'instar du propos précédent autour des OSE, une concertation entre l'autorité de contrôle et les ministères concernés débouchant sur un avis autour des solutions technologiques applicables à la vidéocaptation comme des infrastructures assimilables à des OIV apparaît opportune.

La qualification de ces infrastructures est d'autant plus nécessaire pour pouvoir définir ce qui relève d'une information pouvant être partagée auprès du public (ex : publication des cartes en ligne situant les dispositifs de vidéocaptation) comme explicité plus en avant dans le document.

2. Délai de conservation

La DPD observe que le projet de position de la CNIL n'aborde pas la question des délais de conservation des données issues de la vidéocaptation « augmentée ».

L'article L.252-5 du Code de la Sécurité Intérieur précise que *« les enregistrements sont détruits dans un délai maximum fixé par l'autorisation. Ce délai ne peut excéder un mois. »*

Ainsi, l'interrogation porte sur les règles existantes en matière de délais de conservation. Les dispositifs de vidéocaptation « augmentée » doivent-ils être assimilés à la vidéocaptation « classique » ?

Ainsi, la DPD estime qu'il serait opportun que la CNIL prenne une position spécifique sur ce sujet étant donné le caractère protéiforme des données et des finalités attribuées.

B. Transfert des données

La Délégation à la protection des données souligne que la question des transferts de données hors de l'UE n'est, à ce stade, pas abordée dans ce projet.

Effectivement, dans le cadre de l'hébergement des données par des prestataires dans le cadre des applications SaaS concernant la surcouche logicielle des dispositifs de vidéocaptation « augmentée », cette problématique pourrait se poser. Par ailleurs, au-delà de l'état du droit actuel, les enjeux de souveraineté numérique sont un élément de plus en plus prégnant dans le débat public comme encore récemment autour du débat concernant le Health Data Hub. Raison pour laquelle la voix de l'autorité de protection des données reste déterminante dans son rôle de conseil auprès des pouvoirs publics.

C. Dimension européenne

Dans le cadre de l'utilisation de la vidéocaptation, le traitement de données provenant de ce type de dispositif peut revêtir un enjeu du traitement hors du territoire national ou encore un traitement transfrontalier des données.

Le traitement hors territoire national ou transfrontalier des données de vidéocaptation vient s'inscrire dans un cadre de coopération avec des pays frontaliers à notre collectivité territoriale pour préserver et améliorer la sécurité des personnes et des biens.

La localisation du traitement initial de données ou encore la transmission de ces données qui peut intervenir entre deux organismes de nationalité différentes impactent potentiellement les personnes en dehors du territoire national français. Nous pouvons également retrouver de tels enjeux dans le cadre des transports pouvant opérer sur le territoire à la fois français et allemand.

Ainsi, la problématique de la géographie du traitement hors de France est un véritable enjeu. Il est donc à envisager que les autorités de contrôle européennes abordent cette question et se positionnent sur ce sujet.

D. Transparence (open data/contrôle démocratique-citoyen)

1. Open-data

La Ville et l'Eurométropole de Strasbourg publient de nombreux documents dans le cadre de l'open data. En principe, l'opportunité de la diffusion des informations au regard de l'intérêt public à connaître de ces informations doit toujours être mis en balance avec la protection des droits et libertés des personnes.

Ainsi, l'intérêt public à connaître les informations concernant les caractéristiques de la vidéocaptation, tel que leur emplacement géographique, en prenant en considération le droit à la sécurité et à la sûreté de nos populations, est un élément de discussion fort. La DPD appelle la CNIL à fournir un conseil fort sur les points d'équilibre à trouver entre nécessité de transparence, risques pour les droits et libertés fondamentaux des personnes concernées comprenant ainsi le droit à la sûreté et à la sécurité des personnes.

Selon les promoteurs des technologies de vidéocaptation, la présence ostensible ou non de caméras tend à réduire les conditions environnementales opportunes aux infractions, rendant l'exécution d'un acte de malveillance plus périlleuse.

Or, la publication publique de l'emplacement géographique précis des dispositifs de vidéocaptation voire de ses caractéristiques techniques peut potentiellement faciliter les atteintes à la sécurité des personnes et des biens.

Un regard spécifique de la CNIL autour de l'open data en lien avec les dispositifs de vidéocaptation « classique » ou « augmentée » paraît dès lors nécessaire en dehors des éléments signalant l'existence du dispositif conformément à sa doctrine.

2. Contrôle démocratique-citoyen

Dans la continuité d'un principe de transparence autour de la mise en place et du fonctionnement de la vidéocaptation, le contrôle démocratique des usagers de la collectivité est essentiel.

Différentes collectivités territoriales ont fait le choix de la mise en place d'un organe de contrôle, nommé « comité d'éthique » ou encore « conseil d'éthique », chargé de veiller au respect des libertés publiques et privées fondamentales en cause. Ce type d'organe a vocation à être tourné vers les usagers par un rôle d'information du fonctionnement de la vidéocaptation. Dans le même temps, il a notamment pour rôle à traiter des réclamations ou toute sollicitation de la part des usagers à ce sujet.

La mise en place, la composition et le fonctionnement de ce type d'organe n'est régit par aucun dispositif normalisé à l'heure actuelle.

Comme l'indique la CNIL, à son point 1.6., l'adoption de cette technologie doit impérativement être considérée au travers de la protection des droits et libertés fondamentaux des personnes. Dans cet esprit, il est nécessaire que l'autorité de contrôle se prononce, en lien avec les ministères concernés, sur l'organisation par les pouvoirs publics d'un contrôle démocratique-citoyen sur les dispositifs de vidéocaptation.

3. Transparence des algorithmes

La transparence des algorithmes est une question centrale aujourd'hui où les technologies sont de plus en plus développées et utilisées par le citoyen, le consommateur ou l'usager des services publics. En effet, avec le développement des outils numériques, nous sommes de plus en plus confrontés à l'automatisation de traitement de ces données.

Concernant le traitement automatisé des données provenant de la vidéocaptation, la CNIL souligne, dans son point 3.1.11., qu'« *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* ».

Ainsi, la notion d'éthique est au cœur de la problématique des algorithmes et de leur transparence, car ces algorithmes ont une importance capitale dans nos modes de vie actuels. La publication des informations concernant les algorithmes contribue à comprendre, évaluer voire de s'opposer à toutes discriminations.

La loi pour une République numérique du 7 octobre 2016 dispose que, suite à toutes décisions administratives prises sur le fondement d'un algorithme, les personnes intéressées ont la possibilité de demander plus de précisions sur cet algorithme et sa logique.

Il est essentiel que la CNIL précise les modalités pratiques visant à la transparence des algorithmes, autrement dit à leur intelligibilité, dans le cadre de la vidéocaptation.

Naturellement, la transparence de l'algorithme ne repose pas sur la diffusion de son code-source. En effet, à moins d'avoir des compétences en matière informatique, ce code ne sera pas plus intelligible

à l'utilisateur. La transparence consisterait donc à une meilleure information et à une explication compréhensible et accessible à tous de la manière dont fonctionne l'algorithme.

L'apport par l'autorité de contrôle d'un cahier de spécifications à mettre en œuvre dans la publication des informations de l'algorithme utilisé dans le cadre du fonctionnement de la vidéocaptation semble ici souhaitable.

I. Remarques et interrogations concernant la partie « Observations préalables » du projet de position

Dans cette partie la DPD constate que certains sujets ont été exclus du projet et que certaines problématiques n'ont pas été abordées.

A. Exclusion de certaines technologies

La CNIL se positionne directement quant à l'exclusion de son projet de position de la problématique liée à l'utilisation de la technologie de reconnaissance faciale et biométriques qui sont pourtant bien des dispositifs de caméras « intelligentes » ou « augmentées » et qui sont bien et de plus en plus présents dans ces différents dispositifs. Effectivement, la CNIL avait déjà pris position sur ces sujets spécifiques dans les lignes directrices.

Pour autant, à des fins d'une meilleure lecture entre les différents cadres existants, il semble souhaitable, dans l'intérêt du grand public comme des métiers compétents, que la CNIL reprenne ces positions et les articulent au regard de la présente consultation.

B. Exclusion de certains lieux

La CNIL a pris position de ne traiter que des espaces publics et lieux ouverts au public.

Ainsi, la DPD note que ce projet de position se concentre essentiellement sur le lieu de déploiement de la technologie utilisée. Or, les potentialités technologiques énumérées dans le projet peuvent être applicables précisément dans les espaces non ouverts au public, avec notamment la question de l'utilisation de ces technologies dans le cadre des relations de travail (en lien notamment avec l'article L.2312-38 du code du travail concernant l'information préalable du comité social et économique).

Ces sujets semblent importants en terme d'enjeux pour la protection des données et la DPD appelle à ce que l'autorité de contrôle traite de cette question spécifique.

C. Certains dispositifs particuliers

En vue d'enrichir la portée de sa vision, la CNIL pourrait opportunément traiter de cas particuliers qui pourtant connaissent beaucoup d'exemples et de pratiques concrètes sur le terrain, tel que par exemple les dispositifs caméras portés par les agents de la Police municipale ou encore les dispositifs de vidéocaptation équipant des véhicules ou points fixes (LAPI, etc.).

La DPD est d'avis que le futur projet de l'autorité de contrôle devrait inclure ces dispositifs connus et particulièrement utilisés dans notre société pour en dégager les bonnes pratiques pour l'ensemble des acteurs.

Par ailleurs, la DPD souligne que le projet de position se retrouverait encore plus riche en faisant un focus sur la question des drones qui a suscité de nombreuses critiques et réactions médiatiques et populaires lors de tentatives de contrôle du port du masque ou du respect des mesures de confinement ou couvre-feu à l'occasion de la crise sanitaire du COVID-19.

D. Les biais algorithmiques

Comme l'indique la CNIL dans son projet de position, au point 3.1.11, « *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*. »

La loi pour une République numérique de 2016 a permis de modifier certaines dispositions et d'offrir des garanties : les décisions administratives prises sur la base d'un algorithme peuvent faire l'objet d'un recours qui ne sera pas basé sur un algorithme.

La DPD appelle la CNIL et le Défenseur des Droits à continuer son travail d'actualisation et à émettre des recommandations sur l'articulation des garanties prévues par la loi pour une République numérique avec les possibilités d'usage de la vidéocaptation.

II. Remarques et interrogations concernant la partie 3. « Une technologie porteuse de risques gradués pour les droits et libertés des personnes »

La DPD soulève deux points dans cette partie du projet. Tout d'abord, elle fera un focus sur la notion de proportionnalité dans le cadre de l'évaluation des risques que peuvent engendrer ces caméras « intelligentes » (A), puis mettra en avant la question de l'accès aux données de ces dispositifs (B).

A. Point de précision sur la notion de proportionnalité

Dans le cadre de l'évaluation des risques qu'engendrent ces dispositifs sur les droits et libertés des personnes dont les données sont traitées, la proportionnalité doit être évaluée.

Ce principe de proportionnalité implique que cette technologie ne devrait être utilisée que s'il n'y a pas un moyen moins intrusif pour parvenir au même résultat escompté.

Cependant cette analyse reste encore trop subjective et il existe donc un risque de non uniformisation entre les différentes interprétations que les acteurs peuvent avoir. Ceci pose un problème de cadre juridique non clairement détaillé et peut amener à des utilisations qui ne seront pas proportionnées en fonction de l'interprétation de chacun.

Ainsi, la DPD sollicite l'autorité de contrôle afin que celle-ci pose une grille de lecture concrète, un état de l'art, pour mener cette analyse de la proportionnalité dans le cadre de l'utilisation de ce type de dispositif afin de permettre un cadre clair et uniforme pour tous les acteurs.

B. Point de précision sur la nécessité d'un besoin d'en connaître

L'évaluation des droits et libertés touchés par la vidéocaptation « intelligente » prend également en compte l'accès aux données collectées. Effectivement, plus il est simple d'accéder aux données collectées, moins la protection des données est assurée. En particulier la transmission des flux vidéos aux tiers autorisés est un sujet non abordé dans ce projet de position de la CNIL.

La DPD estime qu'il serait nécessaire d'aborder cette question dans le cadre de cette position de la CNIL. Et ce, notamment concernant l'accès aux flux vidéos par les tiers autorisés, tel que la préfecture ou les autorités assurant des missions de police ou de renseignement. De manière plus précise la DPD se demande si une transmission en temps réel ou en différé est possible et/ou souhaitable.

III. Remarques et interrogations concernant la partie 4. « des conditions de légalité différenciées en fonction des objectifs, des conditions de mise en œuvre et des risques des dispositifs de vidéo « augmentée » »

A. Articulation avec les dispositions CSI (4.1)

Les dispositions du Code de la Sécurité Intérieur (CSI) fixent un cadre applicable à la vidéocaptation traditionnelle (sans couche technologique supplémentaire). La CNIL mentionne que le régime prévu par le CSI n'interdit pas en lui-même toute utilisation de la vidéo « augmentée ».

Ainsi, il apparaît à la lecture du projet de position de la CNIL que le CSI encadre uniquement la vidéocaptation en tant que tel et non la technologie qui intervient dans le cadre de caméra « augmentée ».

La DPD souligne l'absence de précision sur l'utilisation des dispositions du CSI en tant que base légale (condition de licéité) du traitement de données dans le cadre de la vidéo « augmentée ».

En conséquence, la DPD est dans l'attente à ce que la CNIL précise sa position sur la licéité du traitement au moyen de l'encadrement du CSI en détaillant les cas de figure possibles. L'enjeu est d'apporter un éclairage sur les règles d'encadrement juridique de la vidéocaptation « augmentée ».

B. Les principes communs applicables à tous les dispositifs de vidéo "augmentée" (4.2)

4.2.3.

La CNIL mentionne dans ce projet les différents acteurs qu'il peut exister dans le cadre de l'utilisation de ces dispositifs : responsable de traitement, co-responsable de traitement et sous-traitant. Mais il n'y a pas de précisions sur ce sujet.

La DPD sollicite l'autorité de contrôle afin que celle-ci apporte des précisions sur ces différents acteurs. Des exemples des différents rôles ainsi que des détails sur les responsabilités de chacun dans les traitements de données dans le cadre des caméras « intelligentes » seraient les bienvenus.

4.2.4.

La CNIL indique que la finalité doit être déterminée, explicite et légitime conformément à l'article 5.b.1 du RGPD.

Ainsi, il semble opportun que la CNIL précise la notion de « explicite » et « légitime » de manière plus concrète dans le cadre de l'utilisation de ces dispositifs de vidéocaptation « intelligente ».

Afin d'avoir un cadre juridique comme d'éviter toute confusion dans l'interprétation par chacun des responsables de traitement, il serait intéressant de disposer d'une grille de lecture de ces notions spécifiquement dans ce contexte.

4.2.5.

Dans ce paragraphe la CNIL indique que toutes les bases légales du RGPD peuvent potentiellement fonder un traitement relatif à l'utilisation de caméra « intelligente ». Cependant au cours du développement, seul le critère de licéité relatif à l'intérêt légitime est détaillé. Le consentement fait lui l'objet que d'une simple indication.

Ainsi, la DPD estime nécessaire d'explorer les possibilités offertes par d'autres bases légales au sein du présent projet. Effectivement, dans le 4.3 du projet, il est uniquement fait mention de la base légale « traitement nécessaire au respect d'une obligation légale » (article 6.1.c du RGPD).

La DPD est également d'avis qu'il est nécessaire de faire appel au législateur pour donner une assise juridique adéquate au regard de cette technologie afin de permettre d'avoir une base légale appropriée.

En outre, l'autorité de contrôle donne exclusivement des exemples dans lesquels l'intérêt légitime ne pourrait pas servir de base.

Il semble ainsi utile que la CNIL indique également des cas d'exemple où l'intérêt légitime et le consentement serait possible pour une mise en place d'un système de vidéocaptation « augmentée » afin d'avoir une vision plus lisible de ces bases légales.

Enfin, la DPD entend à ce que l'autorité de contrôle, et plus particulièrement le CEPD, prenne une position affirmée sur l'exclusion de l'intérêt légitime comme fondement juridique pour ce type de traitement.

Dès lors, comme indiqué dans son article 4.3, l'intérêt légitime apparaît comme un fondement inadéquat au vu du non-respect du droit d'opposition des personnes concernées. Cela plaiderait en faveur d'une absence de déploiement de ces dispositifs.

4.2.6.

Concernant la notion de proportionnalité, il est indispensable que la CNIL se positionne sur la méthodologie à adopter pour opérer la mise en balance les atteintes potentielles à la vie privée et les droits fondamentaux des personnes concernées par le traitement.

Il sera opportun d'apporter aux responsables de traitement une grille de lecture pour analyser la proportionnalité en fonction de la base légale du traitement et de critères d'analyse complémentaire ayant trait à la protection de la vie privée (par exemple : selon les catégories de personnes concernées).

4.2.7.

La DPD s'interroge autour du contenu et des moyens de l'information à donner aux personnes concernées sur l'existence de ce traitement : les informations obligatoires de l'article 13 et 14 du RGPD sont-elles suffisantes ? Sont-elles adaptées ? Doit-on également préciser l'analyse effectuée par la surcouche logicielle aux personnes concernées ? Jusqu'à quel degré de précision devons-nous donner cette information ? Comment s'assurer de la lisibilité et de la compréhension de cette information ?

Ainsi, la DPD enjoint l'autorité de contrôle d'indiquer précisément quelles sont les informations obligatoires que le responsable de traitement devrait délivrer lorsqu'il recourt à un tel dispositif de vidéocaptation « augmentée ».

La DPD requiert de la part de l'autorité de contrôle des précisions sur les différents supports que les responsables de traitement pourraient mettre en œuvre. Ces indications porteraient sur le type de support avec une distinction selon les catégories de personnes concernées par le dispositif afin d'assurer une information accessible.

4.2.8.

La CNIL précise dans ce projet de position que les analyses d'impacts relatives à la vie privée, réalisées dans le cadre des « traitements mis en œuvre par une autorité compétente et à des fins de prévention et de détection des infractions pénales », doivent faire l'objet d'une consultation obligatoire de la CNIL.

La DPD propose d'élargir ce spectre ouvrant une consultation obligatoire de la CNIL sur l'analyse d'impact relative à la vie privée effectuée dans le cadre de l'utilisation de vidéocaptations « augmentées ». Ainsi, il serait bénéfique que l'autorité de contrôle indique également d'autres cas et exemples où cette consultation de la CNIL serait obligatoire.

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

Si le constat de départ autour de la problématique et des enjeux exposés est partagé, la DPD estime nécessaire une plus grande pédagogie autour du cadre juridique qui régira ce type de dispositif, raison d'être du futur projet de positionnement de la CNIL en vue d'assurer notamment une sécurité et une garantie juridique face à la prolifération des caméras intelligentes.