S'agissant de l'AIPD en général

L'analyse effectuée dans son ensemble apparait incomplète dans la mesure où les développements ne traitent pas de l'intégralité du traitement vidéo, mais seulement de certaines fonctionnalités de celui-ci.

Comme l'a rappelé la CNIL sur son site internet, il s'agit de considérer en premier lieu le dispositif vidéoprotection en tant que traitement susceptible de rendre nécessaire la réalisation d'une AIPD.

De par son ampleur et ses conditions d'exploitation, le traitement vidéoprotection de la ville de Marseille apparaît devoir faire l'objet d'une AIPD sur le fondement du RGPD (article 35-1) et/ou de la directive police-justice (obligation transposée à l'article 90 de la loi informatique et libertés).

Le sujet de l'encadrement juridique exige également davantage de précision afin de pouvoir déterminer avec précision le ou les régimes applicables et les conséquences sur le traitement (les réponses à certaines questions devront être adaptées en conséquence).

S'agissant de la finalité du traitement

La première finalité apparait insuffisamment précisée dans la mesure où l'analyse se limite à décrire une fonctionnalité (l'alerte au regard de situations « anormales ») sans préciser le ou les objectifs poursuivis par l'ensemble du dispositif. Il convient donc d'aborder dans l'AIPD la ou les finalités de l'ensemble du dispositif vidéo en veillant en particulier à assurer leur caractère déterminé et explicite. Ces développements pourront faire état d'exemples, de cas d'usage et d'utilisation de fonctionnalités spécifiques afin d'illustrer ces finalités.

S'agissant plus précisément de la mention de la seconde finalité (« *raccourcir les temps de recherche des évènements signalés sur réquisition de la police nationale* »), il convient de préciser que la nécessité de répondre à des réquisitions ne peut être le fondement d'une finalité d'un traitement. En raison notamment du périmètre fluctuant par nature de ces actes, une telle finalité ne peut en effet satisfaire à l'exigence de détermination prévue à l'article 5-1-b du RGPD et 4-1-b de la Directive police).

S'agissant des acteurs sous-traitants et fournisseurs de solution

Les sociétés XXX sont présentées comme sous-traitantes au sens de l'article 28 du RGPD.

Le détail de leurs interventions dans les opérations de traitement de données à caractère personnel n'apparaissent cependant pas explicitement au sein de l'AIPD (ni dans le cycle de vie des données, ni dans le schéma réseau par exemple). Il convient de décrire précisément les opérations réalisées par chacun de ces acteurs sur les données (rôle, étapes et modalités de traitement, circuit des échanges, type d'accès etc.) et de les inclure en conséquence dans le cycle de vie et dans le schéma réseau précité. Il conviendra à cette occasion de préciser le fonctionnement ainsi que les modalités d'intégration des solutions XXX au sein du système d'information (de la ville de Marseille ou des sous-traitants).

S'agissant de la base légale et des référentiels applicables invoqués

L'AIPD précise, dans la partie « *Quels sont les fondements qui rendent votre traitement licite ?* », que le fondement du traitement est « *l'obligation légale par la Ville de Marseille d'assurer la sécurité des citoyens conformément au CGCT* » en citant l'article L. 2212-2 du CGCT.

Bien que ce développement ne comporte pas de référence au RGPD, la collectivité semble donc prévoir la mise en œuvre de l'article 6-1-c du Règlement (« *le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis* »).

Cette mention apparaît insuffisamment justifiée dans la mesure où la CNIL a pu préciser, concernant l'article 6-1-c du RGPD, que « *le recours à cette base légale se justifie lorsque la mise en œuvre d'un traitement est imposée à un organisme par des textes européens ou nationaux* ». En l'espèce la seule invocation de l'article précité du CGCT ne peut suffire dans la mesure où la disposition précitée n'a pas pour effet d'imposer aux collectivités de mettre en œuvre un dispositif de vidéoprotection. Il convient par conséquent de compléter ce développement (le cas échéant en identifiant une autre base légale, telle que celle prévue à l'article 6-1-e du RGPD si le traitement devait, pour partie ou en totalité, s'y conformer).

Par ailleurs, le paragraphe relatif aux « référentiels applicables » ne fait pas état, parmi les textes cités, du RGPD. Il convient par conséquent de s'assurer que les développements « base légale » et « référentiels applicables » sont cohérents.

Enfin, les réflexions menées à ce sujet devront prendre en compte les précisions apportées par la collectivité au sujet de la ou des finalités poursuivies par la vidéoprotection. Certaines finalités, en fonction des modalités de mise en œuvre, pourront en effet donner lieu à retenir le cadre juridique de la directive (UE) 2016/680 « police-justice » (la CNIL propose une distinction des régimes par finalités usuellement poursuivies), et par conséquent de ses dispositions.

S'agissant des données traitées

L'AIPD précise que les données traitées sont « *certains flux vidéos issus des vidéos captés par les caméras* ». Il convient de rappeler que les données à caractère personnel ne peuvent se réduire à un support. Il convient d'énumérer dans l'AIPD les différentes informations à caractère personnel faisant l'objet du recueil et de l'analyse algorithmique.

En cohérence avec la remarque initiale (cf. « S'agissant de l'AIPD en général ») cette description devra être menée au regard de l'ensemble du dispositif vidéo et non seulement des fonctionnalités d'analyse d'image.

Les précisions devront notamment être apportées s'agissant du contexte de recueil des images et des fonctionnalités précitées. Il pourra s'agir par exemple de précisions relatives :

- aux types de lieux filmés (ex. voie publique, certains bâtiments municipaux ou lieux particuliers, angles choisis)
- aux types de données recueillies et, le cas échéant, interprétées (ex. image de la personne, silhouettes, catégorie d'âge, sexe, déplacements, comportement, franchissement de ligne, participation à un attroupement, type de véhicule, immatriculation, comportement de conduite)
- aux données de contexte associées aux images (ex. horodatage, localisation, déclenchement d'une alerte, etc.)

À ce sujet, les éléments d'information fournis à la CNIL détaillant le fonctionnement des solutions fournies par XXX devront être précisées (ex. les fonctionnalités effectivement retenues devront être isolées parmi celles mentionnées dans la brochure commerciale transmise).

S'agissant d'une fonctionnalité en particulier, la « recherche sur une personne », il convient d'expliciter précisément son fonctionnement au regard notamment de la possibilité de donner lieu au traitement de données sensibles (le cas échéant via un gabarit biométrique).

Pour rappel l'identification d'une personne au moyen d'une ou plusieurs données sensibles donnerait lieu à l'application des dispositions aussitôt applicables en la matière (notamment article 9 du RGPD et 88 de la loi du 6 janvier 1978 modifiée). La confirmation selon laquelle le dispositif vidéo ne traite aucune donnée sensible à des fins d'identification ou d'analyse permettrait de préciser ce point.

S'agissant du caractère adéquat, pertinent et limité des données

L'AIPD avance que « *le nombre de critères est limité au strict nécessaire pour répondre aux finalités légales* ». Cet élément n'est pas de nature à justifier le caractère adéquat, pertinent et justifié de chaque information traitée par le dispositif vidéoprotection.

D'une part, cette analyse doit être étendue à l'ensemble du dispositif (notamment en abordant le nombre de caméras, les considérations ayant conduit déterminer leur implantation, leur niveau d'efficacité connu à ce jour).

D'autre part, il conviendra d'analyser l'adéquation et la pertinence des données pour chaque outil (algorithme) de qualification des comportements et situations. Cette analyse est de nature à permettre l'évaluation de l'utilité attendue au regard des finalités. Elle pourra être menée en illustrant le cas échéant par des situations concrètes (ex. en quoi la fonction de franchissement de ligne est-elle adéquate et pertinente ? de regroupement de personne ? dans quels types de cas ?).

S'agissant de l'information et des droits des personnes concernées

Il convient d'intégrer dans l'AIPD les mentions d'information destinées aux personnes concernées ainsi que des précisions relatives aux modalités de diffusion de cette information (ex. information par panneaux, nombre de panneaux, diffusion via la presse locale, les réseaux sociaux etc.).

S'agissant des droits, leurs modalités de mise en œuvre ne sont pas abordées autrement qu'en précisant que les personnes peuvent contacter à cette fin le standard de la mairie ou l'adresse « dpo@marseille.fr ».

À ce sujet, une analyse doit être réalisée quant aux droits applicables en fonction de la base légale (ou des bases légales) retenue pour le traitement. Dans un second temps, la mise en œuvre pratique de ces droits pourrait être précisée (s'agissant par exemple du droit d'accès, pour lequel une procédure adaptée pourrait être prévue afin de gérer la problématique des délais de conservation particulièrement courts).

S'agissant de la conservation des données

Le développement relatif à la durée de conservation des images (10 jours) doit :

- Préciser le départ de cette durée (ex. « à compter du recueil par la collectivité »)
- Justifier le délai établi
- Davantage préciser le cas d'allongement de la durée lors d'une réquisition (ex. « *le temps nécessaire à la remise aux autorités* »)

La justification de la durée de conservation des traces (20 ans, « *délai qui s'appuie sur le délai de prescription des crimes pour les cas généraux* ») doit être enrichie en illustrant par exemple via des cas d'usages envisagés ou des précédents en la matière.

S'agissant de la gestion des risques

De manière globale, l'ensemble de la partie « Risques » est traitée de manière trop succincte. Les développements ne permettent pas d'obtenir une connaissance globale et contextualisée ni des risques, ni des mesures censées les traiter.

S'agissant de l'évaluation du risque de l'accès illégitime (confidentialité) :

- hormis l'atteinte à la réputation et le changement de comportement, l'AIPD ne mentionne pas de préjudice ni d'impact sur la vie privée ni sur les droits et libertés (est seulement cité un « *sentiment* » d'atteinte ou un « *sentiment* » de préjudice) ;
- par ailleurs en conclusion la gravité du risque est jugée importante en raison d'un « *impact moral* (…) *important* ». Cette partie doit être approfondie, afin notamment d'envisager les autres types impacts (corporels, matériels) et d'illustrer chacun d'eux.

S'agissant de l'évaluation du risque de la modification non désirée (intégrité) :

- remarque identique à propos de l'approche par la notion de « sentiment » ;
- le risque d'atteinte à l'intégrité des informations de contexte (ex. modification de l'horodatage) doit également être évalué ;
- « sécurisation de l'exploitation » n'est pas une mesure suffisamment précisée ;
- Remarque identique à propos de l'approche par la notion d'impacts exclusivement « moraux ».

S'agissant de l'évaluation du risque de la perte non désirée (disponibilité) :

- Les risques liés aux pertes de possibilité ou obstacle pour d'agir en justice sont à prendre en compte (ex. impossibilité d'ester, de se défendre) ;
- Certaines mesures ne sont pas suffisamment précises (« contrôle des accès logiques ») ni en lien avec le sujet (« sécuriser » / « conserver ») ;
- Il pourrait être envisagé de procéder à la sauvegarde des données sur un support distinct (ou bénéficiant d'accès restreints) ;
- La gravité devra être le cas échéant réévaluée au regard des nouveaux risques et mesures identifiés.

Sur chacun de ces points, il pourra être pertinent de se reporter au guide CNIL « Les bases de connaissance » (accessible depuis le site internet de la CNIL).

Sur les mesures correctives

S'agissant des mots de passe, il apparaît opportun de mentionner que leur gestion s'inscrira dans le cadre établi par la recommandation de la CNIL relative aux mots de passe (Délibérations n° 2017-012 du 19 janvier 2017 et n° 2017-190 du 22 juin 2017) ou, en cas de suivi d'un autre référentiel, de préciser et justifier la politique de gestion des mots de passe.

S'agissant de la gestion des droits, il convient de préciser davantage :

- les différents paramétrages prévus en termes de niveau de droit d'accès (ex. droit accès aux images en direct, droit d'accès aux enregistrements, droits d'accès en d'extraction)
- la politique d'attribution de ces droits

S'agissant des mesures correctives, il convient de préciser si la mise en œuvre du traitement s'accompagnera effectivement ou non des mesures indiquées (ex. la formulation « Les portables des opérateurs pourraient être consignés » ne permet pas de déterminer ce point).

Autres remarques

Sur la demande d'avis des personnes concernées

S'agissant de l'information selon laquelle la collectivité n'a pas demandé l'avis des personnes concernées, il convient à titre liminaire de souligner qu'en raison des enjeux que représente un tel traitement sur les finalités poursuivies et les droits et libertés d'un ensemble large de personnes, le recueil de l'avis des personnes concernées apparaît revêtir un intérêt certain. Une telle consultation permettrait notamment d'enrichir utilement les éléments de réflexion sur différents aspects abordés au sein de l'AIPD.

En l'espèce l'AIPD précise que l'avis n'a pas été demandé dans la mesure où les personnes concernées auraient été « *largement informées* » au moyen de la presse, de la possibilité de consulter un recours devant un tribunal et de l'activité d'information d'associations de défense du droit. Au regard de ces éléments, l'AIPD précise qu'en conséquence les personnes « *ont pu exprimer leur avis de manière publique* ».

Il convient de rappeler à ce sujet que les lignes directrices concernant l'AIPD adoptées le 4 avril 2017 (et modifiées le 4 octobre 2017) prévoient que « *le responsable de traitement doit justifier toute décision de ne pas recueillir l'avis des personnes concernées s'il juge la démarche inappropriée* ».

En l'espèce la seule mention de l'existence d'un contentieux et de travaux de tiers (journalistes et association) ne permet pas d'établir que les personnes concernées ont été mises en mesure de donner leur avis en application de l'article 35-9 du RGPD. Aux fins de justification de cette décision, il convient a minima de préciser les éléments objectifs permettant de considérer que :

- les personnes concernées ont été en mesure de prendre connaissance du dispositif dans son intégralité,
- les personnes concernées ont été informées de la possibilité d'adresser un avis à la collectivité,
- la collectivité a procédé à la revue des avis éventuellement transmis.

Sur la sous-traitance

L'AIPD fait référence à la signature par les sous-traitants XXX d'engagements de confidentialité. Sur un développement ultérieur, il est fait état de la « *contractualisation d'une clause RGPD et son annexe RGPD avec le sous-traitant* ». La transmission à la CNIL de ces actes est nécessaire aux fins de consultation des clauses retenues relatives aux modalités de traitement des données à caractère personnel (clauses prévues aux articles 28 du RGPD, 96 de la loi informatique et libertés modifiée et 132 du décret n° 2019-536 du 29 mai 2019).

Sur l'accès aux images par les services de la DDSP

L'AIPD précise que le réseau informatique de la police municipale fait l'objet d'une « *interconnexion avec le réseau CIVIP de la DDSP* ». Si cette interconnexion devait concerner le traitement vidéoprotection, en préciser les modalités au sein de l'AIPD (notamment sur les droits dont bénéficient les services de police : consultation en direct des images, extraction, paramétrage-réception des alertes, utilisation des fonctions de recherche sur les enregistrements, nombre de caméras concernées etc.).

Sur le calendrier de mise en œuvre des nouvelles fonctionnalités

Précisez, le cas échéant, si un calendrier prévisionnel de mise en service (ou de test) des fonctionnalités a été établi à ce jour.

Précisez également si ce calendrier prévoit le terme (le cas échéant un bilan d'étape) des fonctionnalités algorithmiques (dans la mesure où l'AIPD fait état du fait que les algorithmes font l'objet d'une « *expérimentation* »).