Délibération 2022-045 du 31 mars 2022

Commission Nationale de l'Informatique et des Libertés
Nature de la délibération : Avis
Etat juridique : En vigueur
Date de publication sur Légifrance : Samedi 29 octobre 2022
NOR : CNIX2228921X

Délibération n° 2022-045 du 31 mars 2022 portant avis sur un projet d'arrêté portant autorisation de traitements automatisés de données à caractère personnel destinés à la sécurisation et au contrôle des personnes dans les lieux de rétention administrative (VidéoCRA) (demande d'avis n° 21005490)

La Commission nationale de l'informatique et des libertés,

Saisie par le ministre de l'intérieur d'une demande d'avis concernant un projet d'arrêté portant autorisation de traitements automatisés de données à caractère personnel destinés à la sécurisation et au contrôle des personnes dans les lieux de rétention administrative (VidéoCRA) ;
Vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (RGPD) ;
Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment les I et IV de son article 31 et son titre III ;

Après avoir entendu le rapport de Mme Sophie LAMBREMON, commissaire, et les observations de M. Benjamin TOUZANNE, commissaire du Gouvernement,

Emet l'avis suivant :

La Commission nationale de l'informatique et des libertés (ci-après la Commission) a été saisie par le ministère de l'intérieur d'un projet d'arrêté portant autorisation de traitements automatisés de données à caractère personnel provenant de dispositifs de vidéosurveillance installés dans les emprises des locaux et centres de rétention administrative (LRA et CRA) ainsi que des zones d'attente (ZA) relevant de la compétence de la police et de la gendarmerie nationales, dénommé VidéoCRA.

A titre liminaire, la Commission prend acte des précisions apportées par le ministère selon lesquelles une doctrine d'emploi sur l'utilisation des caméras est actuellement en cours de rédaction par la direction centrale de la police aux frontières qui assure la maîtrise d'œuvre de ce projet.

Sur les finalités et le régime juridique applicable

En premier lieu, s'agissant des finalités poursuivies par les traitements projetées, l'article 1er du projet d'arrêté mentionne que *ces traitements ont pour finalités :*

- *de vérifier le respect des règles de sécurité ;*
- *d'assurer la sécurité de ces lieux et des personnes présentes en vérifiant que ces personnes sont soit retenues, soit autorisées à y accéder, en détectant et en constatant les évènements susceptibles d'entrainer des atteintes au bon ordre, à la sécurité publique ou à la sécurité des personnes ;*
- *de collecter des preuves dans le cadre des procédures judiciaires, administratives ou disciplinaires* .

L'analyse d'impact relative à la protection des données (AIPD) transmise précise que les règles de sécurité dans les centres de rétention administrative, visées à l'article 1er du projet d'arrêté, sont celles mentionnées dans l'arrêté du 28 octobre 2016 pris en application de l'article R. 553-9 du code de l'entrée et du séjour des étrangers et du droit d'asile (CESEDA). Cet arrêté prévoit un modèle de règlement intérieur des locaux de rétention administrative. A cet égard, la Commission considère que la finalité relative à la vérification du respect des règles de sécurité mentionnée à l'article 1er du projet d'arrêté devrait être précisée afin de mentionner le texte qui fait référence aux règles de sécurité visées.

En deuxième lieu, s'agissant du régime juridique applicable aux traitements, la Commission rappelle que, dans la mesure où les dispositifs vidéo seront installés dans les emprises des locaux et centres de rétention administrative ainsi que des zones d'attente relevant de la compétence de la police et de la gendarmerie nationales, il s'agit de dispositifs de vidéosurveillance car ces derniers filment des lieux non ouverts au public. A ce titre, le code de la sécurité intérieure, qui régit les dispositifs de vidéoprotection filmant la voie publique ou des lieux ouverts au public, n'est pas applicable en l'espèce et seules les dispositions de la loi du 6 janvier 1978 modifiée et du RGPD encadrent la mise en œuvre de tels traitements.

Le ministère considère que les traitements relèvent du régime de la directive (UE) 2016/680 du 27 avril 2016 (directive police-justice), transposée au titre III de la loi du 6 janvier 1978 modifiée, dans la mesure où les finalités poursuivies

s'inscrivent notamment dans la mission de protection des menaces contre la sécurité publique.

Cependant, la Commission rappelle que la directive police-justice s'applique aux traitements de données à caractère personnel effectués par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces.

En l'espèce, la Commission rappelle que le placement en centre ou en lieu de rétention est indépendant de toute qualification pénale. Elle relève en outre que le contrôle du respect des règles de sécurité du règlement intérieur de chaque local de rétention administrative (1° de l'article 1er du projet d'arrêté) et des règles de contrôle d'accès (2° de l'article 1er du projet d'arrêté) ne relève pas non plus d'une finalité pénale. Il en va de même de la finalité relative à la collecte de preuves dans le cadre des procédures administratives et disciplinaires (3° de l'article 1er du projet d'arrêté). En revanche, les missions de maintien de la sécurité publique par les forces de l'ordre au sein des centres et lieux de rétention sont susceptibles de relever de la directive précitée. La Commission considère dès lors que les traitements projetés devraient relever d'un régime mixte (RGPD et directive police-justice tel que transposée au titre III de la loi du 6 janvier 1978 modifiée) en fonction des finalités poursuivies.

En troisième lieu, dans la mesure où les traitements sont mis en œuvre pour le compte de l'Etat, intéressent la sécurité publique et ont notamment pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sécurité, les traitements sont autorisés par un arrêté ministériel pris après avis de la CNIL sur le fondement du I de l'article 31 de la loi du 6 janvier 1978 modifiée.

En outre, le projet d'arrêté constitue, en application du IV de l'article 31 de la loi du 6 janvier 1978 modifiée, un acte réglementaire unique. A ce titre, chacun des responsables de traitement (la direction générale de la police nationale, la direction générale de la gendarmerie nationale et la préfecture de police) est tenue d'adresser un engagement de conformité à la CNIL. L'AIPD transmise ayant été réalisée par la direction générale de la police nationale, la CNIL prend acte de ce que cette AIPD vaut engagement de conformité pour ce responsable de traitement.

Enfin, une seule et même AIPD portant sur un ensemble d'opérations de traitement similaires (AIPD cadre) a été transmise à la CNIL, conformément à l'article 90 de la loi du 6 janvier 1978 modifiée.

Sur les données collectées

Les données collectées sont les images captées par les caméras, dans les zones mentionnées à l'article 2 du projet d'arrêté.

En premier lieu, la Commission prend acte des précisions apportées par le ministère selon lesquelles, d'une part, les caméras ne filmeront pas les abords des emprises des LRA et CRA ni des parties de la voie publique, et d'autre part, les caméras filmeront et enregistreront en continu, de jour comme de nuit.

En deuxième lieu, l'AIPD transmise précise qu'il n'y aura pas de collecte de données sensibles au sens de l'article 6 de la loi du 6 janvier 1978 modifiée. La Commission relève qu'un enregistrement vidéo n'est pas considéré en soi comme relevant d'une catégorie particulière de données à caractère personnel. Elle rappelle que si les images font l'objet d'un traitement spécifique sur des données sensibles, l'article 6 de la loi précitée serait susceptible de s'appliquer.

En outre, l'article 2 du projet d'arrêté précise que les lieux d'intimité ainsi que *les lieux dédiés aux échanges couverts par le secret professionnel ne peuvent être filmés* . La Commission prend acte des précisions apportées par le ministère selon lesquelles ces lieux comprennent les chambres, les sanitaires, l'unité médicale (infirmerie), les locaux de l'Office français de l'immigration et de l'intégration (OFII), les locaux syndicaux, les locaux des associations intervenantes dans les CRA, et les locaux dédiés aux visites des familles, des avocats et des représentants des autorités consulaires étrangères. Elle prend également acte de ce que la rédaction dans le projet d'arrêté sera modifiée afin d'indiquer que les lieux d'intimité comprennent notamment les chambres. En outre, la Commission invite le ministère à prévoir, dans la mesure du possible, que les caméras ne filment pas les accès aux lieux d'intimité et aux lieux dédiés aux échanges couverts par le secret professionnel.

Le ministère a indiqué que la hauteur, l'inclinaison et l'occultation physique des caméras par l'ajout de panneaux permettant d'occulter les lieux d'intimité empêcheront toute captation d'image de l'intérieur des bâtiments par les caméras en extérieur et permettront d'assurer le respect de la vie privée des personnes placées en rétention. La Commission souligne qu'une doctrine d'emploi devra intégrer ces éléments.

Toutefois, elle relève que le projet d'arrêté prévoit que seront notamment filmées les zones d'accueil, à l'exclusion de celles réservées au personnel, les espaces de promenade à l'air libre ainsi que les zones d'activités collectives affectées aux personnes retenues. Ces lieux constituent les lieux de vie dans lesquels les personnes retenues sont amenées à passer une partie importante, si ce n'est la majorité, de leur temps en rétention. Elle prend acte des précisions apportées par le ministère de ce que, dans ces espaces, le nombre de caméras devra être limitée et adaptée à taille du CRA, au nombre de personnes retenues et aux risques présentés par les personnes retenues (par exemple, rétention préalable à une expulsion liée à des activités à caractère terroriste).

En troisième lieu, la Commission relève que selon le ministère, les dispositifs de vidéosurveillance ne procèdent à aucune captation sonore. La Commission rappelle que l'interdiction de toute captation sonore constitue une garantie pour la protection de la vie privée des personnes concernées. Elle prend acte que le projet d'arrêté n'autorise que la captation d'images, à l'exclusion de toute captation sonore.

En dernier lieu, la Commission relève qu'en application des articles L. 741-4 et L. 741-5 du CESEDA, des personnes vulnérables et des mineurs peuvent être placés en rétention. Elle appelle donc à une vigilance toute particulière s'agissant du traitement des données de ces personnes.

Sur la durée de conservation des données

L'article 3 du projet d'arrêté indique que les données sont conservées pendant un délai maximum de quatre-vingt-dix jours à compter du jour de leur enregistrement. Au terme de ce délai, ces données sont effacées automatiquement des traitements. Lorsque les données ont, dans le délai de conservation prévu, été extraites et transmises pour les besoins d'une procédure judiciaire, administrative ou disciplinaire, elles sont conservées selon les règles propres à chacune de ces procédures.

La Commission relève que cette durée correspond à la durée maximale de rétention administrative (hors régime spécifique pour les activités à caractère terroriste pour lequel la durée maximale de rétention administrative est de 210 jours), alors même que la durée de rétention de droit commun est de quarante-huit heures. Elle observe également que dans le cadre d'autres traitements sur la mise en œuvre de dispositifs de vidéosurveillance similaires en matière pénitentiaire (l'arrêté du 13 mai 2013 concernant les locaux et établissements de l'administration pénitentiaire, l'arrêté du 23 décembre 2014 concernant les cellules de protection d'urgence et l'arrêté du 9 juin 2016 concernant les cellules de détention), la durée maximale de conservation des données a été fixée à un mois.

Si le ministère indique que les problématiques dans les lieux de détention sont différentes de celles en rétention, il n'apporte pas d'éléments justifiant une conservation plus longue des données alors même que les durées de rétention sont particulièrement courtes.

La Commission prend acte des précisions apportées par le ministère selon lesquelles cette durée de quatre-vingt-dix jours sera réduite à un mois dans le projet d'arrêté.

Sur les droits des personnes concernées

A titre liminaire, dans la mesure où la Commission considère que les traitements projetés devraient relever d'un régime mixte (RGPD et directive police-justice tel que transposée au titre III de la loi du 6 janvier 1978 modifiée) en fonction des finalités poursuivies, elle invite le ministère à mettre en cohérence l'article 5 du projet d'arrêté portant sur les droits des personnes concernées avec le régime juridique applicable.

S'agissant de l'information des personnes concernées, le II de l'article 5 du projet d'arrêté prévoit que *les personnes susceptibles d'être filmées sont informées de l'existence d'un dispositif de vidéosurveillance et des modalités d'accès, de rectification, d'effacement et à la limitation des données par affiches apposées à l'entrée des lieux mentionnées à l'article 1er où sont mis en œuvre ces traitements . Dans un souci de lisibilité, la Commission estime que le II de l'article 5 du projet d'arrêté devrait être complété afin de mentionner qu'il s'agit des modalités d'exercice des droits d'accès, de rectification, d'effacement et à la limitation du traitement* . En outre, la Commission prend acte des précisions apportées par le ministère selon lesquelles les affiches seront traduites dans les six langues onusiennes.

En outre, l'AIPD transmise précise que conformément à l'article 104 de la loi du 6 janvier 1978 modifiée, les personnes seront informées par une publication sur le site web du ministère de l'intérieur. La Commission relève toutefois qu'aucun accès à Internet depuis les centres ou lieux de rétention administrative n'est prévu par le ministère. De plus, l'AIPD précise que les agents de la police et de la gendarmerie nationales seront informés qu'ils peuvent être filmés par un dispositif de vidéosurveillance, ainsi que de leurs droits, par une note de service établie localement par le chef de CRA, de LRA ou de ZA, en plus de l'affichage.

Par ailleurs, le III de l'article 5 du projet d'arrêté prévoit que *conformément aux articles 104 à 106 de la loi du 6 janvier 1978 susvisée, les droits d'information, d'accès, de rectification, d'effacement et à la limitation des données s'exercent directement auprès du responsable ou du chef d'établissement* . A cet égard, la Commission rappelle que l'article 104 de la loi du 6 janvier 1978 modifiée, s'il ne prévoit pas que l'information soit fournie individuellement à chaque personne en cas de collecte directe, impose au responsable de traitement de la *mettre à disposition* des personnes, de façon permanente et sans demande de leur part. Elle attire donc l'attention sur le fait que la rédaction du projet d'arrêté selon lequel le droit à l'information *s'exerce directement auprès* du responsable ou du chef d'établissement semble inappropriée dans la mesure où les informations doivent être mises à disposition des personnes concernées, notamment par voie d'affiches et par la publication sur le site web du ministère de l'intérieur.

Enfin, une information claire et appropriée devra être proposée aux personnes vulnérables en rétention, et notamment aux mineurs.

Sur les mesures de sécurité

Si la Commission prend acte du cloisonnement du réseau dédié aux enregistreurs ainsi que des restrictions d'accès qui pèsent sur l'accès aux serveurs, elle recommande cependant au ministère, au regard de la nature des données, que celles-ci fassent l'objet de mesures de chiffrement conformes à l'annexe B1 du référentiel général de sécurité. Elle prend bonne note de l'usage d'outil de chiffrement adéquat pour l'extraction des vidéos.

En outre, la Commission prend note de l'usage d'horodatage dans les flux vidéo ainsi que de l'ajout, lors de l'extraction d'un filigranage numérique (*watermarking*) de la vidéo et d'une signature numérique pour empêcher toute modification du contenu. Elle conseille au ministère de préciser dans la doctrine d'emploi que cette signature devrait utiliser un algorithme conforme à l'annexe B1 du référentiel général de sécurité. Elle invite par ailleurs le ministère à conseiller l'usage généralisé de filigranage numérique lors de la consultation pour décourager toute copie optique des enregistrements.

La Commission accueille favorablement la présence dans la doctrine d'emploi d'une politique de mots de passe respectant ses recommandations pour les nouvelles installations, et d'une revue pour mise à niveau des installations existantes. Les opérateurs en charge du visionnage des images utilisent pour cela un compte générique. Bien que les risques induits par cet usage puissent apparaître faibles au regard des droits limités des opérateurs et des mesures participants à la traçabilité de leur présence, la Commission rappelle qu'elle recommande l'usage systématique d'un compte individuel.

Enfin, la Commission prend acte de la mise en place d'une journalisation. Elle accueille favorablement la restriction d'accès aux données de traçabilité au seul administrateur système, afin de garantir l'intégrité des données de journalisation. De plus, des mécanismes effectifs permettent d'assurer une traçabilité des profils opérateurs (tenue d'une main courante, accès à la salle de consultation par usage de carte agent individuelle et contrôle vidéo de l'accès à la salle). La Commission rappelle que la mise en œuvre de mesures de contrôle des données de journalisation contribue à la sécurité du traitement par la génération d'alertes, et prend note que ce contrôle fait partie des missions des conseillers informatique et libertés ainsi que du correspondant informatique local.

La présidente,
M.-L. Denis