

Délibération n° 2025-022 du 10 décembre 2025

de l'Autorité de Protection des Données Personnelles portant avis sur la consultation du Président du Conseil National relative au projet de Loi relative à l'utilisation de la vidéoprotection et de la vidéosurveillance des lieux accessibles au public pour la détection, la recherche et l'identification des personnes recherchées ou signalées au moyen de système d'identification biométrique à distance

Vu la Constitution du 17 décembre 1962 ;

Vu la Convention de sauvegarde des Droits de l'Homme et des Libertés Fondamentales du Conseil de l'Europe du 4 novembre 1950 ;

Vu la Convention n° 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et son Protocole d'amendement adopté par le Comité des Ministres le 18 mai 2018 ;

Vu le Code Pénal ;

Vu le Code de Procédure Pénale ;

Vu la Loi n° 1.565 du 3 décembre 2024 relative à la protection des données personnelles ;

Vu la Loi n° 1.566 du 3 décembre 2024 portant approbation et ratification du Protocole d'amendement à la Convention 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la Loi n° 1.430 du 13 juillet 2016 portant diverses mesures relatives à la préservation de la sécurité nationale ;

Vu la Loi n° 1.039 du 26 juin 1981 concernant le placement et la protection des malades mentaux ;

Vu l'Ordonnance Souveraine n° 11.327 du 10 juillet 2025 portant application de la Loi n° 1.565 du 3 décembre 2024 relative à la protection des données personnelles ;

Vu l'Ordonnance Souveraine n° 3.153 du 19 mars 1964 relative aux conditions d'entrée et de séjour des étrangers dans la Principauté ;

Vu l'Arrêté Ministériel n° 2017-576 du 19 juillet 2017 portant application de l'article 5 de la Loi n° 1.430 du 13 juillet 2016 portant diverses mesures relatives à la préservation de la sécurité nationale ;

Vu l'Arrêté Ministériel n° 2019-330 du 15 avril 2019 portant application de l'article 6 de la Loi n° 1.430 du 13 juillet 2016 portant diverses mesures relatives à la préservation de la sécurité nationale, créant un traitement d'informations nominatives dénommé « *Fichier central de Police et d'antécédents judiciaires* » ;

Vu l'Arrêté Ministériel n° 2019-333 du 15 avril 2019 portant application de l'article 6 de la Loi n° 1.430 du 13 juillet 2016 portant diverses mesures relatives à la préservation de la sécurité nationale, créant un traitement d'informations nominatives dénommé « *Fichier des personnes recherchées ou signalées* » ;

Vu les Lignes directrices sur la reconnaissance faciale du Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la délibération n° 2015-75 du 29 juillet 2015 de la Commission de Contrôle des Informations Nominatives portant avis sur la consultation du Ministre d'Etat relative au projet de Loi portant diverses mesures relatives à la préservation de la sécurité nationale ;

Vu la délibération n° 2017-040 du 15 mars 2017 de la Commission de Contrôle des Informations Nominatives portant avis sur la consultation du Ministre d'Etat relative aux projets d'Arrêtés Ministériels portant application des articles 5, 7, 8, 10, 12, 15, et 16 de la Loi n° 1.430 du 13 juillet 2016 portant diverses mesures relatives à la préservation de la sécurité nationale ;

Vu la délibération n° 2017-188 du 15 novembre 2017 de la Commission de Contrôle des Informations Nominatives portant avis sur la consultation du Ministre d'Etat relative aux projets d'Arrêtés Ministériels portant application de l'article 6 de la Loi n° 1.430 du 13 juillet 2016 portant diverses mesures relatives à la préservation de la sécurité nationale ;

Vu la délibération n° 2020-151 du 4 novembre 2020 de la Commission de Contrôle des Informations Nominatives portant avis sur le projet de Loi relative à la protection des données personnelles ;

Vu la délibération n° 2021-260 du 1^{er} décembre 2021 de la Commission de Contrôle des Informations Nominatives portant avis sur le projet de Loi relative à la protection des données personnelles ;

Vu la saisine du Ministre d'Etat en date du 9 février 2023 concernant un projet de Loi relative à l'utilisation de la vidéoprotection et de la vidéosurveillance des lieux accessibles au public pour la détection, la recherche et l'identification des personnes recherchées ou signalées au moyen de système d'identification biométrique à distance ;

Vu la délibération n° 2023-066 du 26 avril 2023 de la Commission de Contrôle des Informations Nominatives portant avis sur la consultation du Ministre d'Etat relative au projet de Loi relative à l'utilisation de la vidéoprotection et de la vidéosurveillance des lieux accessibles au public pour la détection, la recherche et l'identification des personnes recherchées ou signalées au moyen de système d'identification biométrique à distance ;

Vu le projet de Loi n° 1087 relative à l'utilisation de la vidéoprotection et de la vidéosurveillance des lieux accessibles au public pour la détection, la recherche et l'identification des personnes recherchées ou signalées au moyen de système d'identification biométrique à distance ;

Vu la saisine du Président du Conseil National en date 8 octobre 2025 reçue le 10 octobre 2025 concernant le projet de Loi relative à l'utilisation de la vidéoprotection et de la vidéosurveillance des lieux accessibles au public pour la détection, la recherche et l'identification des personnes recherchées ou signalées au moyen de système d'identification biométrique à distance.

L'Autorité de Protection des Données Personnelles,

Préambule

La Commission de Contrôle des Informations Nominatives (CCIN) a eu connaissance dès 2019 de la volonté du Gouvernement de doter la Direction de la Sûreté Publique (DSP) d'un système d'identification biométrique à distance en temps réel, lorsque Monsieur le Conseiller-Ministre de l'Intérieur était venu l'informer qu'un Arrêté Ministériel pris en application de l'article 6 de la Loi n° 1.430 portant diverses mesures relatives à la préservation de la sécurité nationale serait publié pour donner en droit interne une base légale permettant le recours à cette technologie. Elle a su à cette occasion que la DSP testait un logiciel de reconnaissance faciale en temps réel en dehors de tout cadre légal, sur son système de vidéoprotection urbaine.

La CCIN avait alors indiqué qu'un Arrêté Ministériel ne pouvait être une base légale adéquate pour encadrer une matière aussi sensible et potentiellement attentatoire aux droits et libertés fondamentaux, et le Gouvernement a validé devant le Conseil National, lors de la séance publique budgétaire du 12 décembre 2019, la nécessité de légiférer. A cet égard, SEM Serge TELLE, alors Ministre d'Etat, indiquait qu'« *il ne s'agit pas pour le Gouvernement de Son Altesse Sérénissime de s'engager sur une piste aussi porteuse ou attentatoire aux libertés publiques, en fonction de l'utilisation qui pourrait être faite de cette technologie, sans avoir eu au préalable un débat qui nous permette d'encadrer l'usage de cette technologie avec les dispositions juridiques nécessaires et indispensables donc voilà pour le cadre, je réponds à la question qui m'a été posée oui, nous passerons par la Loi* ».

La CCIN avait finalement été saisie par le Ministre d'Etat en date du 9 février 2023 d'un projet de Loi relative à l'utilisation de la vidéoprotection et de la vidéosurveillance des lieux accessibles au public pour la détection, la recherche et l'identification des personnes recherchées ou signalées au moyen de système d'identification biométrique à distance.

Cette saisine avait conduit à l'adoption de la délibération n° 2023-066 du 26 avril 2023 relative audit projet de Loi. Cet avis n'était pas public, en application des dispositions de la Loi n° 1.165 citée en visa.

Le projet de Loi a ensuite été légèrement modifié par le Gouvernement avant d'être déposé sur le bureau du Conseil National le 19 décembre 2023 et enregistré sous le numéro 1087.

Depuis, la législation monégasque relative à la protection des données personnelles a évolué avec l'adoption de la Loi n° 1.565 du 3 décembre 2024 relative à la protection des données personnelles, parue au Journal de Monaco du vendredi 13 décembre 2024. A cette occasion, l'Autorité de Protection des Données Personnelles (APDP) s'est substituée à la CCIN et peut être, en application de l'article 38 de cette Loi, « (...) consultée par le Président du Conseil National lors de l'étude de propositions de loi ou de projets de loi relatives à la protection des données à caractère personnel ou au traitement de telles données ».

Ainsi, par courrier daté du 8 octobre 2025, le Président du Conseil National a fait part à l'APDP que la Commission de Législation, qui a débuté l'étude du projet de Loi n° 1087, souhaiterait connaître son avis quant au dispositif projeté, si possible, en raison d'impératifs liés au calendrier législatif, avant le mercredi 17 décembre 2025. Cet avis, objet de la présente délibération fera, en application de la Loi n° 1.565, susvisée, l'objet d'une publication sur le site Internet du Conseil National et sur celui de l'APDP.

Entre la saisine initiale du Ministre d'Etat et la présente saisine par le Conseil National se sont écoulées deux années intenses en matière de développement de l'intelligence artificielle (IA), tant au niveau européen que mondial, et il est opportun de résumer les évolutions survenues dans cet intervalle.

Aussi, avant d'analyser le projet de Loi n° 1087 et la situation monégasque, une contextualisation s'impose quant au recours à ce type de technologies de par le monde et leur encadrement par les pays de l'Union européenne.

Pour rappel, lorsque la CCIN a été saisie du projet de Loi en 2023, il existait alors des discussions avancées au sein de l'Union européenne concernant l'encadrement de l'Intelligence Artificielle par un Règlement européen, qui n'était pas encore dans sa version finalisée. La prise en compte par l'opinion publique de l'Intelligence Artificielle était émergente avec la montée en puissance qui s'amorçait des outils d'Open AI, Mistral puis le développement des IAs génératrices de vidéo.

Concernant la reconnaissance faciale en Europe, la plupart des dispositifs sont sanctionnés par les Autorités de contrôle de protection des données, bien qu'une utilisation très encadrée de cette technologie est permise *a posteriori* dans le cadre d'investigations criminelles.

Au niveau international, outre la Chine et son système de notation sociale, il existe toutes sortes de situations, entre promotion de la technologie et son interdiction à San Francisco (à l'exception des aéroports et des sites fédéraux) ou son autolimitation par des acteurs de la technologie comme Axon qui refuse de déployer la technologie sur les caméras portatives de la police. Relevons toutefois que la police de l'immigration américaine commence à utiliser la reconnaissance faciale de force lors d'interpellations au faciès, renouvelant aux Etats-Unis les inquiétudes quant aux modalités d'utilisation de cette technologie et relançant le débat public sur la nécessité d'encadrer ou d'interdire son usage.

Au Canada, le Commissariat à la Protection de la vie Privée, à l'issue de son enquête et rapport spécial parlementaire portant sur la Gendarmerie royale du Canada, a estimé que l'utilisation de la technologie de reconnaissance faciale par la police pourrait être permise uniquement si on peut préalablement montrer son efficacité pour chaque usage particulier. Il y écrit que : *« les services de police ne devraient pas avoir recours à la technologie de reconnaissance faciale tout simplement parce que l'on estime qu'elle est "utile" pour l'application de la loi de manière générale. Les services de police doivent avoir un motif précis de faire appel à cette technologie et ce motif doit être fondé sur des éléments probants. Il ne suffit pas de s'appuyer sur des objectifs généraux en matière de sécurité publique pour justifier l'utilisation d'une technologie aussi intrusive. Le caractère urgent et important de l'objectif en question devrait être démontrable par des éléments probants »*.

Le Règlement européen sur l'Intelligence Artificielle 2024/1689 du 13 juin 2024 (AI ACT) est entré en vigueur le 1er août 2024 avec une application progressive au sein de l'Union européenne à partir de février 2025, soit après le dépôt du projet de Loi n° 1087. Il convient d'en exposer la portée avant d'étudier *stricto sensu* le projet de Loi n° 1087, notamment dans l'appréhension des droits et libertés fondamentaux de l'UE dont Monaco

souhaite qu'elle reconnaisse l'adéquation de sa législation en matière de protection des données personnelles.

Ce texte européen classe l'utilisation de système d'identification biométrique à distance en temps réel dans des espaces accessibles au public à des fins répressives parmi les pratiques interdites en matière d'IA (article 5 §1 h)).

Toutefois, le même texte précise des exceptions à cette interdiction en indiquant que le recours à ce type de système est possible si l'utilisation est strictement nécessaire eu égard à l'un des objectifs suivants :

- « i) la recherche ciblée de victimes spécifiques d'enlèvement, de la traite ou de l'exploitation sexuelle d'êtres humains, ainsi que la recherche de personnes disparues ;
- ii) la prévention d'une menace spécifique, substantielle et imminente pour la vie ou la sécurité physique de personnes physiques ou d'une menace réelle et actuelle ou réelle et prévisible d'attaque terroriste ;
- iii) la localisation ou l'identification d'une personne soupçonnée d'avoir commis une infraction pénale, aux fins de mener une enquête pénale, d'engager des poursuites ou d'exécuter une sanction pénale pour des infractions visées à l'annexe II et punissables dans l'État membre concerné d'une peine ou d'une mesure de sûreté privatives de liberté d'une durée maximale d'au moins quatre ans ».

De plus il est précisé au paragraphe 2 du même article que cette technologie ne doit être déployée « *que pour confirmer l'identité de la personne spécifiquement ciblée et tient compte des éléments suivants :*

- a) *la nature de la situation donnant lieu à un éventuel recours au système, en particulier la gravité, la probabilité et l'ampleur du préjudice qui serait causé si le système n'était pas utilisé ;*
- b) *les conséquences de l'utilisation du système sur les droits et libertés de toutes les personnes concernées, notamment la gravité, la probabilité et l'ampleur de ces conséquences ».*

En outre, l'utilisation de ce type de système doit également respecter « *les garanties et conditions nécessaires et proportionnées en ce qui concerne cette utilisation, conformément au droit national qui l'autorise, notamment eu égard aux limitations temporelles, géographiques et relatives aux personnes* ». Il est par ailleurs important de procéder également à une analyse d'impact conformément à l'article 27 du RGPD et d'enregistrer le système conformément à l'article 49 de l'AI ACT.

Par ailleurs, chaque utilisation à des fins répressives du système est soumise à l'autorisation par une Autorité judiciaire ou une Autorité Administrative Indépendante dont la décision est contraignante. L'autorisation est délivrée sur demande motivée après analyse de la nécessité et de la proportionnalité au regard des cas où l'utilisation est autorisée avec notamment la limitation « *dans le temps et du point de vue de la portée géographique et personnelle* ».

Il est en outre indiqué au paragraphe 4 de l'article 5 que l'Autorité de protection des données ainsi que l'Autorité de surveillance du marché doivent être notifiées de « *toute utilisation d'un système d'identification biométrique à distance en temps réel dans des espaces accessibles au public à des fins répressives* ».

Enfin, conformément au paragraphe 5 du même article chaque Etat Membre doit prévoir des règles en droit interne au sujet de l'utilisation de ce type de système : cas d'utilisation (dans la limite de celles de l'AI ACT), les règles détaillées nécessaires à la demande, à la délivrance et à l'exercice des autorisations, ainsi qu'à la surveillance et à l'établissement des rapports, les infractions pénales concernées, etc. Ces règles doivent ensuite être transmises dans un délai de 30 jours après leur adoption à la Commission.

Concernant la mise en œuvre de ce type de système utilisant des données biométriques à des fins répressives dans un contexte Police/Justice, il semblerait que le cadre de l'AI ACT se substitue à l'article 10 de la Directive Police/Justice, qui encadre de manière exhaustive cette utilisation et le traitement des données biométriques qui en résulte. De plus, il est précisé que l'AI ACT ne constitue pas une base juridique pour le traitement des données personnelles en application de l'article 8 de la Directive (considérant 38 de l'AI ACT).

Enfin, tout traitement de données biométriques et d'autres données personnelles *« mobilisées lors de l'utilisation de systèmes d'IA pour l'identification biométrique, qui n'est pas lié à l'utilisation de systèmes d'identification biométrique à distance en temps réel dans des espaces accessibles au public à des fins répressives »* doit rester conforme aux exigences de l'article 10 de la Directive, et de l'article 9 § 1 du RGPD.

Pour rappel, même l'accueil d'un événement aussi sensible en termes de sécurité que les Jeux Olympiques de Paris n'a pas donné lieu au recours à de la reconnaissance faciale identifiant des personnes en temps réel, mais au recours à des scénarios d'événements détectés par un algorithme. Relevons à cet égard que le recours à des caméras algorithmiques n'était permis à titre expérimental que jusqu'au 31 mars 2025 et que la Commune de Montrouge a dû arrêter un système de ce genre qu'elle exploitait illégalement après cette date.

Pour finir ce tour d'horizon, voici quelques situations actualisées dans le droit interne de certains pays européens.

En France, 2 propositions de Loi sont en cours d'analyse :

- la première en date du 12 juin 2023 émane du Sénat et définit les grands principes relatifs à l'utilisation de la reconnaissance biométrique dans l'espace public avec notamment l'interdiction de toute catégorisation et notation des personnes physiques ; la prohibition de l'identification biométrique réalisée à distance qu'elle soit en temps réel ou *a posteriori* ; la nécessité de l'obtention du consentement des personnes concernées. Cette proposition de Loi fixe également un cadre pour l'expérimentation de traitements de données biométriques. La Commission des Lois du Sénat exposant la nécessité de l'adoption préalable d'une Loi d'expérimentation *« pour créer le débat et déterminer les usages de la reconnaissance biométrique qui pourraient être pertinents et efficaces. L'expérimentation pourrait être autorisée pour une période de trois ans, ce qui obligerait le Gouvernement et le Parlement à réévaluer le besoin et recadrer le cas échéant le dispositif en fonction des résultats obtenus »*. Cette Mission du Sénat a également précisé que *« pour que cette phase d'expérimentation soit utile, serait mise en place une évaluation publique et indépendante pour connaître l'efficacité de la technologie dans le cas d'usage testé. Elle serait conduite par un comité composé de scientifiques et de spécialistes des questions éthiques dont les rapports seraient rendus publics »* ;
- la seconde en date du 17 avril 2025 émane de l'Assemblée Nationale et vise à interdire la reconnaissance faciale en contestant l'efficacité de la vidéosurveillance pour lutter ou prévenir la criminalité (98% des attentats empêchés en France entre 2013 et 2019 l'ont été grâce aux renseignements humains).

La Loi sur la fonction de police de la Belgique prévoit la possibilité pour les Services de police de traiter certaines données biométriques pour assurer une identification unique (article 44/1). Toutefois, cette identification biométrique ne semble pouvoir être réalisée qu'avec le consentement de la personne concernée, ou si ces données sont rendues publiques par elle, ou pour protéger les intérêts vitaux de cette personne ou d'une autre personne. Enfin, une proposition de Loi est en cours d'analyse dans le pays depuis le 17 décembre 2024 qui comporte une application avec des précisions de l'AI ACT notamment sur le contenu de l'autorisation délivrée ou encore les infractions concernées.

Au Luxembourg, le Ministre de l'Intérieur ainsi que celui de la Justice ont affirmé en septembre 2025 que si le Gouvernement se montre en principe ouvert aux technologies innovantes, l'utilisation de la reconnaissance faciale automatique en complément des méthodes existantes dans le cadre des enquêtes et de la prévention, n'est pas prévue. Interrogés sur un éventuel projet de texte dans le domaine ils ont précisé « *Un éventuel projet pilote dans ce domaine n'est envisageable que dans le respect de conditions juridiques, techniques et éthiques strictes. Toute approche pratique doit respecter les droits fondamentaux et garantir la proportionnalité* ». Actuellement, la Loi sur la police du Luxembourg exclut en son article 43bis (5) « *Le recours à des techniques de reconnaissance faciale* ».

La Suisse ne dispose pas d'un cadre légal fédéral en matière de reconnaissance faciale mais il y a une tendance à l'interdiction locale. Ainsi, en mai 2025 Lausanne a interdit l'utilisation de la reconnaissance faciale dans l'espace public afin de garantir une certaine liberté dans la ville. Toutefois, cette interdiction ne s'applique pas aux enquêtes menées par la police judiciaire.

Concernant la Principauté, l'APDP estime que le projet de Loi n° 1087 pose difficulté, d'une part eu égard aux problèmes légaux préexistants en droit interne dans lequel il vient s'insérer, d'autre part eu égard à la qualité intrinsèque dudit projet.

I. Sur les problèmes structurels ne permettant pas un déploiement serein de la reconnaissance faciale en Principauté

A) Sur l'insécurité juridique résultant de l'encadrement légal de la vidéoprotection et de la vidéosurveillance en Principauté

En France, filmer les lieux ouverts au public est une prérogative de puissance publique et la vidéoprotection ne peut être mise en œuvre que par des Autorités publiques ou, sur autorisation de l'Autorité préfectorale, par des personnes privées qui justifient d'un intérêt (protéger les biens et les personnes à l'intérieur d'un commerce, filmer les abords immédiats d'un bar qui a connu plusieurs incidents, etc.), étant précisé que la proportionnalité du dispositif est appréciée par une Commission de vidéoprotection présidée par un Magistrat.

Le Gouvernement monégasque s'est inspiré de ces dispositions françaises quand il a introduit en droit interne la vidéoprotection par le biais de l'article 5 de la Loi n° 1.430. Toutefois, il a limité le domaine de la vidéoprotection aux seules Autorités publiques compétentes, en substituant au régime d'autorisation prévu en France pour les personnes privées un régime d'autorisation ouvert aux seules Autorités publiques compétentes.

Ce choix a principalement eu pour effet de rendre illégale toute installation de système vidéo par une entité privée dans un lieu ouvert au public, créant des situations juridiquement intenable pour de nombreuses sociétés.

Pour corriger cela, en lieu et place d'une modification de l'article 5 de la Loi n° 1.430 et donc du régime d'autorisation d'installation d'un système de vidéoprotection, il a été fait le choix d'introduire au sein de la Loi n° 1.565 une section dédiée aux « *traitements relatifs à la vidéosurveillance* », aux termes de laquelle il a été instauré un système de demande d'autorisation au Ministre d'Etat lorsqu'une entité veut installer un système de vidéosurveillance dans un lieu ouvert au public.

Il est donc compliqué, voire dans certaines situations impossible, de comprendre ce qui relève de la vidéoprotection ou de la vidéosurveillance. Les responsables de traitement sont en effet confrontés à deux régimes d'autorisation du Ministre d'Etat dépendant de deux régimes juridiques différents mais qui s'intéressent à une seule et même typologie de lieu relevant d'un même périmètre (non défini) : « *les lieux ouverts au public* ». Par exemple, quel régime doit-on appliquer à la gare ferroviaire ou aux caméras de la Société des Bains de Mer filmant la place du casino ?

Pour tenter de pallier à la difficulté que les textes ont créée, il est intéressant de noter que le projet de Loi n° 1087 prévoit d'ajouter un alinéa 5 à l'article 5 de la Loi n° 1.430 qui dispose que :

« Les images des systèmes de vidéoprotection mis en œuvre par toute autorité administrative autre que la Direction de la Sûreté Publique, peuvent être mises à disposition de ladite Direction au moyen des équipements et liens techniques destinés à y pourvoir dans les conditions prévues par arrêté ministériel »,

et un article 5 bis qui dispose que :

« Les images des systèmes de vidéosurveillance, autorisés par le Ministre d'Etat, installés dans les lieux ouverts au public ou filmant les abords de voies publiques, d'espaces ouverts au public ou à la circulation du public, sont mises à disposition de la Direction de la Sûreté Publique au moyen des équipements et liens techniques destinés à y pourvoir dans les conditions prévues par arrêté ministériel »,

ce qui parfait la démonstration que l'on parle effectivement d'une même typologie de lieux, lieux qui procèdent d'une même nécessité pour la DSP, et permet donc d'en conclure que le double régime actuel est artificiel et source d'insécurité juridique.

Il convient également de relever qu'en ce qui concerne la vidéosurveillance présente au sein de la Loi n° 1.565, et le régime d'autorisation du Ministre d'Etat y associé, il est prévu que « *Les modalités d'application de la présente section sont définies par Arrêté Ministériel* ».

Ce dernier n'a, près d'un an après l'entrée en vigueur de la Loi n° 1.565, pas été soumis à l'avis de l'APDP et donc, n'a pas été publié. L'Autorité estime qu'il doit être difficile d'adopter un texte différent de l'Arrêté Ministériel n° 2017-576 du 19 juillet 2017 portant application de l'article 5 de la Loi n° 1.430 du 13 juillet 2016 portant diverses mesures relatives à la préservation de la sécurité nationale, qui prévoit en son article premier l'autorisation du Ministre pour les systèmes de vidéoprotection. Or, une duplication du régime à la vidéosurveillance ne ferait que renforcer le caractère factice entre ce qui relève d'une vidéosurveillance et d'une vidéoprotection des lieux ouverts au public.

L'APDP rappelle en outre que l'autorisation délivrée par le Ministre d'Etat devrait se borner à une acceptation de principe à la mise en œuvre par un responsable de traitement d'un système de vidéo filmant un lieu ouvert au public, comme délégation d'une prérogative de puissance publique, et ne devrait en aucun cas procéder d'une appréciation de la proportionnalité du système. Elle appelle donc à trouver un équivalent à la Commission de vidéoprotection qui en France, présidée par un Magistrat, apprécie la proportionnalité du

système, ou à réintroduire auprès de l'APDP un régime d'autorisation concernant ce type de dispositif.

A cet égard, par le passé, il a été constaté par l'Autorité une incitation à l'installation de davantage de caméras que nécessaire auprès des entités sollicitant l'autorisation des systèmes par le Ministre d'Etat pour filmer les lieux ouverts au public. S'il semblerait que dans l'attente de l'Arrêté Ministériel d'application de la Loi n° 1.565 relatif à la vidéosurveillance, il ne soit plus procédé à la revue des systèmes soumis à autorisation (en gelant également la délivrance des autorisations au secteur privé), la tendance à la sur-installation de caméras pourrait être renforcée si l'Arrêté Ministériel d'application attendu confiait l'appréciation de la proportionnalité du dispositif à la DSP, qui y trouverait un nouvel intérêt si elle disposait en plus du droit de s'y interconnecter. Cela créerait en outre une insécurité juridique pour les responsables de traitement, car l'APDP demeure garante du contrôle de ces dispositifs et pourrait sanctionner le déploiement d'un système trop intrusif.

En tout état de cause, il est difficile de comprendre sur quelles caméras la DSP peut nativement introduire la technologie d'identification biométrique à distance et celles sur lesquelles les images peuvent lui être mises à disposition.

B) Sur les limites créées par les choix opérés lors de l'adoption de la Loi n° 1.565

a) Les traitements relevant des articles 9 à 15 et 18 de la Loi n° 1.430 n'entrent pas dans le champ de compétence de l'APDP

L'article 8-3 projeté mentionne en son alinéa 1-4° que le Directeur de la DSP établit « *une liste d'alerte portant sur les personnes recherchées ou signalées au titre de la poursuite des finalités énoncées au deuxième alinéa de l'article 9* », à savoir :

« 1°- la prévention du terrorisme, de la criminalité et de la délinquance organisées ainsi que de la prolifération des armes de destruction massive ;

2°- la défense des intérêts stratégiques de la politique extérieure de la Principauté, le respect de ses engagements internationaux, ainsi que la prévention de toute forme d'ingérence étrangère ;

3°- la sauvegarde des intérêts fondamentaux suivants de la Principauté : le maintien de son indépendance et de ses institutions, l'intégrité de son territoire, la sécurité et la sauvegarde de sa population, ainsi que la protection des éléments essentiels de son potentiel scientifique et économique ».

L'article 37 alinéa 4 de la Loi n° 1.565 dispose que « *Sont exclus de la compétence de l'autorité (...) 2. les traitements intéressant la sûreté de l'État et la sécurité nationale régis par les dispositions des articles 9 à 15 et 18 de la loi n° 1.430 du 13 juillet 2016 portant diverses mesures relatives à la préservation de la sécurité nationale qui relèvent de l'autorité de contrôle spécifique formée par la Commission Spéciale de Sécurité Nationale instituée par l'article 16 de ladite loi, et qui sont contrôlés au regard de la réglementation en vigueur en matière de données personnelles conformément aux dispositions de la Section VII du Chapitre VII de la présente loi* ».

Dès lors, l'APDP ne peut vérifier cette liste d'alerte. Toutefois, la Commission Spéciale de Sécurité Nationale (CSSN) ne le peut pas non plus car :

- le traitement de vidéoprotection et le contrôle du système d'identification biométrique à distance relèvent des prérogatives de l'APDP ;
- ce contrôle est en tout état de cause hors de son champ d'investigation prévu à l'article 16 de la Loi n° 1.430, très restreint, qui dispose que « *De sa propre initiative ou sur réclamation de toute personne y ayant un intérêt direct et personnel, la Commission*

peut procéder au contrôle de toute mesure d'interception ou de recueil d'informations, en vue de vérifier si elle est effectuée dans le respect des dispositions de l'article 14. La Commission notifie à l'auteur de la réclamation que les vérifications nécessaires ont été effectuées, sans jamais confirmer ou infirmer la mise en œuvre de l'une des opérations de police administrative visées au présent titre. Les dispositions du huitième alinéa sont applicables ».

Ainsi, la liste d'alerte « portant sur les personnes recherchées ou signalées au titre de la poursuite des finalités énoncées au deuxième alinéa de l'article 9 », et l'utilisation qui en serait faite par le système d'identification biométrique à distance en temps réel, sont totalement incontrôlables, privant les personnes concernées de tout recours effectif quant au respect de leurs droits et libertés fondamentaux.

La présence d'informations relevant de l'article 9 au sein d'une liste d'alerte a également pour conséquence :

- soit que l'ensemble des agents utilisant la vidéoprotection sont habilités secret de sécurité nationale ;
- soit qu'il existe un déport au sein de la Division du Renseignement Intérieur, rendant encore plus compliqué tout éventuel contrôle.

L'APDP estime *a priori* que toute solution différente d'un retrait de cette liste d'alerte ou d'une refonte de l'article 37 de la Loi n° 1.565 serait bancal et juridiquement fragile.

b) Le choix inopportun de dispenser les traitements relevant de la Police/Justice d'analyses d'impact

Les textes européens exigent que soit démontrée au préalable la « *nécessité absolue* » de tout traitement biométrique de surveillance, et les lignes directrices sur la reconnaissance faciale du Comité Consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel de la Convention 108, à laquelle Monaco est Partie, expliquent notamment que « *si elles envisagent le déploiement des technologies de reconnaissance faciale dans des environnements non contrôlés (NB : ouverts au public), les autorités chargées de l'application de la loi devront :*

- *évaluer et expliquer dans leur évaluation l'absolue nécessité et la proportionnalité du déploiement de ces technologies ;*
- *aborder le risque pour différents droits fondamentaux, notamment pour le droit à la protection des données, à la liberté d'expression, à la liberté de réunion et à la liberté de circulation ou à la lutte contre la discrimination, en fonction des utilisations potentielles en différents endroits ».*

Pourtant, aucun élément justifiant de la nécessité absolue n'est étayé au sein du projet de Loi, et aucune étude sur une appréciation du *ratio* bénéfices attendus / risques d'atteintes aux droits et libertés fondamentaux n'est indexée. Le projet de Loi ne remplit donc pas les critères imposés par les engagements internationaux de la Principauté.

L'APDP relève que ce constat est aggravé car la Loi n° 1.565, à l'inverse du droit européen, dispense de toute analyse d'impact avant de solliciter l'avis de l'APDP relativement à un traitement Police/Justice.

L'analyse d'impact a été jugée superflue par les Services du Gouvernement dès le stade de l'élaboration du projet de Loi au prétexte que l'avis rendu par l'APDP (en application de l'article 58 dans la version définitive du texte) sur de tels traitements suffirait.

Toutefois, cet avis, rendu dans un délai de 2 mois renouvelable une fois, ne peut pas se substituer à des analyses d'impact qui peuvent parfois prendre plus d'une année pour être menées à bien, le temps par exemple d'apprécier véritablement les enjeux juridiques et techniques d'une solution informatique.

Ainsi, en cas de vote d'un texte sur l'analyse biométrique à distance, la DSP pourra saisir pour avis l'APDP lors du déploiement effectif de la reconnaissance faciale sans aucune analyse d'impact. Cette saisine ne serait pas entachée d'irrégularité alors même que le responsable du traitement s'est dispensé d'étudier :

- la qualité et l'éthique de la phase d'apprentissage de l'algorithme soutenant le dispositif de reconnaissance faciale (avec par exemple, l'assurance que les personnes dont les visages servent à l'apprentissage des algorithmes en soient informées et y consentent) ;
- si l'algorithme concerné présente des biais, potentielles sources d'erreurs en raison du genre ou de l'origine ethnique de la personne concernée ;
- sur qui repose le maintien dans le temps de la qualité du dispositif, à savoir la DSP ou l'acteur privé choisi ;
- la nécessité et la proportionnalité de disposer d'une telle technologie en permanence et sur toutes les caméras, sans limitation des usages dans le temps ou selon les lieux et événements ;
- les solutions possibles en cas de problème avec l'éditeur de la solution choisie ;
- la proportionnalité du dispositif sur les personnes vulnérables, le projet de Loi soumis à avis prévoyant notamment que sont concernées « *les personnes qui ne jouissent pas de la plénitude de leurs facultés mentales et qui présentent un risque pour les personnalités de la Famille Princière* » ;
- les seuils de faux positifs et de faux négatifs que le Gouvernement estime acceptables pour préférer une solution à une autre ;
- la nécessité d'un contrôle par un Magistrat avant de placer un individu sur une liste le soumettant à un contrôle continu par reconnaissance faciale.

Or, comme l'indique le Comité Consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel de la Convention 108, dans son analyse du 5 septembre 2019 intitulée « *la reconnaissance faciale : état des lieux et enjeux* », « *Lorsqu'une autorité publique n'a pas encore acquis ou développé un système de reconnaissance faciale, cette évaluation [des risques] devrait être effectuée avant l'acquisition et/ou le développement de cet outil et être rendue publique. De plus, les autorités publiques devraient imposer à tout fournisseur d'outil envisagé une levée de toute restriction à l'échange d'informations si cela a un effet limitant de l'analyse d'impact* ».

L'APDP réitère donc ses demandes de réintroduction au sein de la Loi n° 1.565 de l'obligation pour les traitements dits de Police/Justice de mener à bien une analyse d'impact devant être jointe aux saisines pour avis de l'Autorité ou qu'à *minima* cette obligation soit inscrite dans le présent projet de Loi, s'il devait être adopté, s'agissant du déploiement du dispositif projeté.

En effet, comme démontré, l'analyse d'impact permet d'apporter aux justiciables davantage de garanties s'agissant de la pleine appréhension par l'Etat des conditions assurant le respect de leurs droits et libertés fondamentaux.

c) Le risque d'élargissement des mesures de surveillance par voie réglementaire

L'APDP s'inquiète que tout cadre défini au terme du vote d'une Loi relative à un système d'identification biométrique à distance puisse être constamment élargi par voie

règlementaire, donnant au dispositif une portée que le Conseil National ne pouvait pas anticiper et n'aurait éventuellement pas souhaité lui donner.

A cet égard, il convient de rappeler que la CCIN s'était inquiétée, dès 2021, de la nature des missions confiée à l'Unité Drone et lutte anti-drone nouvellement créée au sein de la DSP. En réponse à ses inquiétudes, le Gouvernement lui avait alors indiqué que *« l'instruction d'emploi de ces matériels proscrit leur utilisation à des fins de contrôle d'identité ou d'identification des personnes »*, précisant toutefois que tout texte réglementaire spécial pourrait être prévu à cet égard.

L'APDP reprend à son compte ces inquiétudes, ayant su de manière fortuite que le Gouvernement réfléchissait à l'élaboration d'Arrêtés Ministériels visant à encadrer la vidéoprotection mobile (dont les drones). Cela élargirait considérablement la portée du présent projet de Loi et des modalités de contrôle qu'étudie le Conseil National si un Arrêté Ministériel permettait *in fine* d'utiliser de manière mobile toute technologie d'identification biométrique à distance en temps réel.

Une inquiétude similaire peut également concerner l'impact d'un éventuel dévoiement de la portée des Décisions Ministérielles prises en application du Règlement Sanitaire International comme la CCIN a pu le constater lors de la récente crise sanitaire, qui pourraient permettre de manière dérogatoire de nouveaux types de contrôles en cas de crise nouvelle (contrôle des températures corporelles par exemple, ou absence de port du masque).

En outre, le cadre légal peut être propice à cette pratique, la Loi n° 1.430 permettant une délégation presque sans limite de prérogatives au pouvoir réglementaire, sans que l'on sache avec certitude s'il est possible pour le Gouvernement d'y recourir eu égard aux dispositions des articles 58 et 64 de la Loi n° 1.565.

En effet, l'article 6 de la Loi n° 1.430 dispose que :

« Pour la bonne exécution de ses missions de police administrative ou de police judiciaire, le Directeur de la Sûreté Publique met en œuvre, dans des conditions prévues par arrêté ministériel, des traitements automatisés d'informations nominatives permettant, notamment, l'identification des personnes et des biens, par tous procédés techniques et moyens informatiques appropriés, dans le respect des dispositions de la loi n° 1.565 du 3 décembre 2024.

Lesdits traitements peuvent faire l'objet d'une interconnexion avec les fichiers des services administratifs concernés, dans le respect des dispositions de la loi n° 1.565 du 3 décembre 2024. »

Enfin, relevons que l'article 77 de la Loi n° 1.565 relatif aux traitements de données à caractère personnel relatifs aux données génétiques ou biométriques dans un contexte police/justice dispose que :

« Les traitements mis en œuvre par les autorités administratives et judiciaires, agissant dans le cadre de leurs prérogatives de puissance publique, qui portent sur des données génétiques ou sur des données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes sont soumis à l'avis de l'autorité de protection dans les conditions prévues à l'article 59.

Ces traitements ne peuvent être mis en œuvre que sous réserve de garanties appropriées pour les droits et libertés de la personne concernée, et de mesures d'organisation et de sécurité adéquates telles que notamment le cloisonnement des données lors de leur transmission et de leur conservation, le stockage séparé des données personnelles brutes et des modèles créés à partir de ces données brutes (...) ».

Il n'exige ainsi pas la recherche d'une nécessité absolue telle que le prévoit le droit européen ou l'article 88 de la Loi informatique et libertés qui dispose que : « *Le traitement de données mentionnées au I de l'article 6 est possible **uniquement en cas de nécessité absolue**, sous réserve de garanties appropriées pour les droits et libertés de la personne concernée, et soit s'il est autorisé par une disposition législative ou réglementaire, soit s'il vise à protéger les intérêts vitaux d'une personne physique, soit s'il porte sur des données manifestement rendues publiques par la personne concernée* ».

Aussi l'APDP ne peut que regretter vivement l'absence de démonstration d'une nécessité absolue, ainsi que l'éventuelle extension par voie réglementaire, qui constitue un risque majeur pour les droits et libertés des personnes concernées, dans un domaine aussi intrusif en matière de préservation de la vie privée.

C) Sur l'état des lieux des traitements de la DSP

L'établissement de listes d'alerte suppose de s'appuyer sur des traitements existants et à jour. Deux traitements prévoient en Principauté l'utilisation de photographies « *notamment celles comportant des caractéristiques techniques permettant de recourir à un dispositif de reconnaissance faciale* », à savoir ceux créés par :

- l'Arrêté Ministériel n° 2019-333 du 15 avril 2019 portant application de l'article 6 de la Loi n° 1.430 du 13 juillet 2016 portant diverses mesures relatives à la préservation de la sécurité nationale, créant un traitement d'informations nominatives dénommé « *Fichier des personnes recherchées ou signalées* » ;
- l'Arrêté Ministériel n° 2019-330 du 15 avril 2019 portant application de l'article 6 de la Loi n° 1.430 du 13 juillet 2016 portant diverses mesures relatives à la préservation de la sécurité nationale, créant un traitement d'informations nominatives dénommé « *Fichier central de Police et d'antécédents judiciaires* ».

Ces deux traitements s'inspirent des traitements équivalents français. Toutefois, il convient de relever quelques différences majeures :

- si le Traitement des Antécédents Judiciaires français (TAJ) permet également de contenir des photographies « *notamment celles comportant des caractéristiques techniques permettant de recourir à un dispositif de reconnaissance faciale* », l'utilisation est limitée à de l'identification *a posteriori* des personnes physiques mises en cause (comparaison entre bases de données), des personnes physiques faisant l'objet d'une enquête ou d'une instruction pour recherche des causes de la mort ou d'une disparition. Cette reconnaissance faciale n'est pas liée à un système d'identification biométrique à distance. Le Conseil d'Etat français précise que « *le dispositif de reconnaissance faciale ne peut être utilisé par les services compétents qu'en cas de nécessité absolue, appréciée au regard des seules finalités du traitement, lorsque subsiste un doute sur l'identité d'une personne dont l'identification est requise* » ;
- le TAJ est codifié dans le Code de Procédure Pénale français, quand les Arrêtés Ministériels précités ne sont pas accessibles sur Legimonaco. Seuls les initiés peuvent

savoir que ces textes sont accessibles uniquement sur le Journal de Monaco, et leur recherche nécessite de connaître au préalable leur existence ;

- il est prévu au sein du TAJ que « *Le traitement des données à caractère personnel est opéré sous le contrôle du procureur de la République territorialement compétent, qui, d'office ou à la demande de la personne concernée, ordonne qu'elles soient effacées, complétées ou rectifiées, notamment en cas de requalification judiciaire, ou qu'elles fassent l'objet d'une mention. (...) La personne concernée peut former cette demande sans délai à la suite d'une décision devenue définitive de relaxe, d'acquiescement, de condamnation avec dispense de peine ou dispense de mention au casier judiciaire, de non-lieu ou de classement sans suite. Dans les autres cas, la personne ne peut former sa demande, à peine d'irrecevabilité, que lorsque ne figure plus aucune mention de nature pénale dans le bulletin n° 2 de son casier judiciaire. En cas de décision de relaxe ou d'acquiescement devenue définitive, les données à caractère personnel concernant les personnes mises en cause sont effacées, sauf si le procureur de la République en prescrit le maintien, auquel cas elles font l'objet d'une mention (...)* ». Il n'existe pas d'équivalent en Principauté.

Ainsi, en Principauté, il n'y a aucune supervision prévue de la qualité des informations. L'APDP a pu constater au cours d'exercices de droits d'accès indirects qu'elle a effectués sur les traitements de police :

- qu'il ne semble y avoir aucune séparation effective entre les différents traitements légalement érigés en Principauté, amalgamant les différentes données personnelles collectées pour différentes finalités et leurs durées de conservation, de manière non conforme aux dispositions légales ;
- que des personnes ayant fait l'objet d'une décision de réhabilitation ou de relaxe demeurent inscrites dans les fichiers de police, car la DSP n'est pas informée de l'évolution de la situation des personnes concernées ;
- qu'il est difficile pour les personnes concernées de corriger cette situation, même avec l'intervention de l'APDP. A titre d'exemple, l'APDP vient de recevoir un an après saisine initiale du Ministre d'Etat par ses soins, et après une après plusieurs relances, une fin de non-revoir à la demande d'effacement d'informations concernant une personne dont l'inscription au sein des traitements de police est pourtant due à une erreur.

Concernant le droit d'accès indirect, l'APDP rappelle que la rédaction des articles 59 et 60 de l'Ordonnance Souveraine n° 11.327 portant application de la Loi n° 1.565, en créant une procédure *contra legem*, ne lui permet plus de procéder à de véritables vérifications au sens de l'article 74 de la Loi n° 1.565.

En outre, depuis l'adoption de la Loi n° 1.430, aucun traitement de « *renseignement* » n'est officiellement mis en œuvre en Principauté. Ainsi, tout traitement en la matière est exploité en dehors de tout cadre légal, étant rappelé que les articles 9 à 15 et 18 de la Loi n° 1.430 encadrent uniquement le recours à des techniques de renseignement par lesquelles s'opèrent certaines collectes de données (délibérations CCIN n° 2015-75, n° 2020-151, n° 2021-260), et non les traitements eux-mêmes.

Dès lors, l'APDP estime qu'en l'état, le risque d'être entré par erreur dans une liste d'alerte ne peut être écarté.

II. Sur les problèmes intrinsèques au dispositif lui même

A) **Sur la différence entre les intentions affichées limitées à une certaine utilisation de la reconnaissance faciale et un projet de Loi qui ne pose pas de limites suffisantes**

L'exposé des motifs résume le projet de Loi en une « *simple automatisation de la recherche d'individus par le biais de la reconnaissance faciale en lieu et place des agents de la DSP* ».

Or, le dispositif ne se limite pas à l'utilisation de la reconnaissance faciale. Le projet de Loi ne définit pas la notion la notion d'« *identification biométrique à distance* » qui ne peut être réduite à une technologie de reconnaissance faciale mais en comprend de nombreuses autres, comme l'analyse de comportements ou de la température des personnes filmées.

A cet égard, dans une interview de décembre 2019 donnée à Monaco Hebdo, Monsieur Jean-Philippe Claret, présenté comme le « *patron de l'entreprise monégasque Confidentia, en charge de l'installation de la reconnaissance faciale en principauté* » car ayant « *remporté l'appel d'offre (...) dont l'installation se monte à un million d'euros* », indiquait :

« *Aujourd'hui, on est capable de détecter un certain nombre de choses. La première utilisation, c'est de pouvoir savoir où se concentre l'œil humain. Ça peut être utilisé aussi sur une personne qui reste longtemps dans un espace où elle ne doit pas rester, avec les yeux orientés trop longtemps vers quelque chose qui n'a pas d'intérêt. Vous considérez que c'est quelqu'un qui est en train de faire quelque chose qu'il n'a pas à faire.* » « *En combinant l'outil visuel que sont les caméras dotées de logiciels de reconnaissance faciale, avec l'outil thermique, l'objet est capable de tout détecter : Vous coupez tous les éléments (élévation de température, transformation du visage) pour en faire un outil qui vous permet de tout détecter. La façon de dialoguer entre outils est maintenant normalisée. [...] Les possibilités techniques de ce genre d'outils sont infinies.* »

Dès lors, la DSP pourrait *in fine* mettre en œuvre n'importe quelle autre technique d'identification biométrique à distance (voire des technologies de police prédictive ...) sans contrevenir au projet de Loi n° 1087, qui n'interdit formellement que la seule mise en œuvre d'un système de notation sociale.

En outre, il n'est pas certain que l'utilisation de cette technologie soit limitée à la DSP, le 10° de l'article 5 ouvrant son utilisation « *aux autorités compétentes* » relativement à la détection d'individus, et donc potentiellement à la Police Municipale par exemple.

De plus, le projet de Loi ne permet pas de dresser la frontière entre ce qui relève d'une utilisation en temps réel et différée de la technologie envisagée, notions qui ne sont pas définies, et qui amalgament donc des recours complètement différents à la technologie (voir supra sur l'utilisation en France de la reconnaissance faciale en utilisant des données du TAJ).

Par ailleurs, il est indiqué au sein de l'exposé des motifs qu'a été apprécié l'équilibre entre la protection des droits des personnes et l'efficacité du dispositif et ainsi, que « *Le Gouvernement Princier a alors pu considérer que de telles garanties étaient de nature à assurer un niveau de protection aussi élevé que possible pour les droits et libertés fondamentaux des personnes concernées par le traitement de données objet du présent projet de loi (...)* ».

Or, outre les différents problèmes énumérés dans la présente délibération, l'APDP relève :

- que le seuil du recours à l'identification biométrique à distance est celui d'une infraction punissable d'un an seulement d'emprisonnement, soit 80% des infractions du Code Pénal. L'APDP estime dès lors qu'un tel ratio ne peut être présenté comme un système à haut risque déployé pour des « *finalités de sécurité impérieuse* », garantie pourtant évoquée par le Gouvernement pour l'appréciation de la proportionnalité du système. Pour rappel, ce seuil concerne au sein de l'AI ACT « *des infractions visées à l'annexe II et punissables dans l'État membre concerné d'une peine ou d'une mesure de sûreté privatives de liberté d'une durée maximale d'au moins quatre ans* » ;
- qu'en cas d'infraction à l'interdiction de mettre en œuvre un tel système biométrique, un des plus attentatoires aux droits et libertés fondamentaux des personnes, les peines encourues sont inférieures aux peines présentes dans le droit commun de la protection des données personnelles. A titre d'exemple, en France, installer un système de vidéoprotection en France de manière induue (sans recours à de la biométrie) est pourtant susceptible de 3 ans de prison (article L. 254-1 Code de la Sécurité Intérieure) ;
- qu'il n'existe aucune sanction d'un usage/accès indu par les personnels de la DSP ni droit à réparation pour les personnes concernées.

De plus, au titre des garanties évoquées par le Gouvernement lors de la saisine de la CCIN, existaient des limites d'usage dans le temps ou à certains lieux (notamment pour les événements sportifs), qui semblaient techniquement impossibles et ont été retirées du présent projet. Cependant, le caractère omniprésent et permanent du dispositif en sort renforcé et la liste des garde-fous s'en trouve diminuée.

Enfin, le texte est silencieux quant à l'obligation d'informer les personnes concernées et les modalités y associées. En effet lesdites personnes doivent savoir qu'elles intègrent un périmètre géographique soumis à l'identification biométrique à distance, dont il est envisagé une mise en œuvre permanente sur l'ensemble du territoire.

B) Sur la problématique de l'établissement des listes d'alerte

L'article 8-3 en projet conduit à l'élaboration de 6 listes d'alertes correspondant en grande partie aux personnes recherchées ou signalées au titre de l'Arrêté Ministériel n° 2019-333, précité, auxquelles s'ajoutent en application de son alinéa 3 les « *personnes signalées ou recherchées à l'étranger pour l'un ou plusieurs des motifs visés aux points 1 à 5 du premier alinéa, lorsque ces personnes font l'objet d'une notice, d'une fiche ou d'une information diffusée ou échangée sur le fondement des traités et accords internationaux auxquels la Principauté est partie, ou dans le cadre des organisations internationales de police ou de sécurité dont elle est membre* ».

A cet égard, il convient de relever que :

- les textes français disposent que « *Sont inscrits dans le fichier des personnes recherchées au titre des décisions judiciaires (...) 1° Les mandats, ordres et notes de recherches émanant du procureur de la République, des juridictions d'instruction, de jugement ou d'application des peines, du juge des libertés et de la détention et du juge des enfants tendant à la recherche ou à l'arrestation d'une personne* » ;
- tandis que l'Arrêté Ministériel n° 2019-333 dispose que « *Peuvent être inscrites dans le traitement visé à l'article premier les personnes recherchées ou signalées au titre (...) 1°) de décisions judiciaires concernant :*

- a) les décisions, mandats, notes ou instructions émanant d'une autorité judiciaire ;
- b) les autres décisions mandats, notes ou instructions émanant d'une autorité judiciaire et qui imposent des mesures de contrôle, de surveillance ou qui tendent à assurer le respect d'obligations particulières » ;
- et le projet de Loi n° 1087 dispose que « le Directeur de la Sûreté Publique établit séparément : 1°) une liste d'alerte portant sur les personnes recherchées ou signalées au titre de décisions, mandats ou instructions émanant d'une autorité judiciaire concernant une infraction punie d'une peine supérieure ou égale à un an d'emprisonnement ».

A titre liminaire, l'APDP constate des différences rédactionnelles entre le projet de Loi n° 1087 et l'Arrêté Ministériel n°2019-333. Ce dernier est source d'insécurité juridique en ce qu'il permet un pouvoir discrétionnaire quant à l'insertion d'une personne dans le traitement (« **Peuvent être** inscrites dans le traitement visé à l'article premier les personnes recherchées ou signalées »).

Mais, surtout, quand en France les personnes concernées sont intégrées au sein du traitement seulement si elles font l'objet d'actes ou décisions « *tendant à [leur] arrestation* », le projet de Loi n° 1087 permet en Principauté d'insérer dans la liste tous types de personnes « *signalées* » au titre d'actes d'une Autorité judiciaire concernant une infraction punie d'une peine supérieure ou égale à un an d'emprisonnement.

L'APDP estime que cette liste pourrait être source d'une interprétation extensive qui permettrait au Directeur de la DSP d'y insérer toute personne liée à une décision d'une Autorité judiciaire concernant une infraction punie d'une peine supérieure ou égale à un an d'emprisonnement, sans qu'elle soit recherchée en vue de son arrestation ni même forcément l'auteur de l'infraction (alors que les témoins et les victimes ne peuvent pourtant pas faire l'objet de mandats de recherche en application du Code de Procédure Pénale). Les personnes faisant l'objet d'un contrôle judiciaire semblent ainsi par exemple pouvoir faire l'objet d'un suivi permanent par la reconnaissance faciale envisagée.

En outre, le projet d'article 8-3 alinéa 1-3. porte en lui les germes d'une utilisation sans limite de la reconnaissance faciale. Il permet en effet d'inscrire sur la « *liste d'alerte* » des personnes recherchées ou signalées au titre « *d'enquêtes diligentées dans le cadre de recherches des causes de la mort, de personnes disparues, de disparitions inquiétantes ou de fugues de mineurs* ». A l'instar des articles 8-3 alinéa1-1. et 8-3 alinéa1-2., il convient de noter qu'il n'est pas précisé quelles catégories de personnes peuvent être recherchées. Rien ne semble interdire à la DSP de porter sur la liste l'ensemble des visages des personnes avec lesquelles la victime a interagi pour connaître également l'ensemble de leurs déplacements. Cette inquiétude est d'autant plus prégnante que la CCIN a pu constater que le logiciel dont la DSP envisageait de se doter incluait la possibilité d'alimenter le système directement par les images issues de la vidéo, permettant en quelque sorte de « *rebondir* » sur des personnes accompagnant une personne recherchée, sans avoir à passer par la « *liste d'alerte* ». Il semble ainsi aisé d'avoir un recours extensif à cette technologie sans qu'il puisse être reproché de contrevenir aux dispositions de la Loi, qui permettent dans cette matière sensible d'en avoir une interprétation très large. Le contrôle par l'APDP d'une utilisation conforme de cette technologie apparaît par avance difficile.

L'APDP constate en outre qu'en application de l'article 22 de l'Ordonnance n° 3.153 du 19 mars 1964 relative aux conditions d'entrée et de séjour des étrangers dans la Principauté, le Ministre d'Etat peut, par mesure de police ou en prenant un Arrêté, expulser de Monaco toute personne qui n'a pas la nationalité du pays et l'interdire d'y pénétrer, et, avec les dispositions projetées, assortir cette décision d'une inscription dans la liste d'alerte afin de soumettre ladite personne à la reconnaissance faciale. Aucune de ces mesures n'est soumise à une procédure préalable contradictoire. Une personne faisant un recours contre une décision

d'expulsion par le Ministre d'Etat et ayant un sauf-conduit pour se faire entendre devant les juridictions sera-t-elle soumise à l'identification biométrique à distance ?

En ce qui concerne les mesures de placement d'office, la CCIN avait relevé des dispositions de la Loi n° 1.039 concernant le placement et la protection des malades mentaux, qu'elles peuvent avoir pour origine soit une décision du Ministre d'Etat, qui transmet le dossier au Procureur Général pour saisine du Tribunal de Première Instance, soit directement en application d'une Ordonnance du Président du Tribunal de Première Instance saisi par le Procureur Général. Aussi, les suites de l'hospitalisation, soumise au contrôle du juge, et la sortie de la personne intéressée par décision du Tribunal, prévue à l'article 12 de ladite Loi, sont inconnues du Ministre d'Etat. L'APDP s'interroge ainsi sur le possible suivi permanent par un système d'identification biométrique à distance d'une personne ayant fait l'objet à un moment de sa vie d'une mesure de placement. Le contrôle périodique de la liste par le Directeur de la DSP semble dès lors inopérant dans cette situation.

Il convient aussi de s'interroger sur la constitution de la liste d'alerte, dont le contenu ressemble en grande partie, pour les catégories de personnes concernées, à une duplication du traitement ayant pour finalité « *Fichier des personnes recherchées ou signalées* ». Ce traitement (ainsi que celui relatif au « *Fichier central de Police et d'antécédents judiciaires* ») permet la collecte de « *photographies et notamment celles comportant des caractéristiques techniques permettant de recourir à un dispositif de reconnaissance faciale* ». Toutefois, le projet de Loi est silencieux quant aux modalités de création de la « *liste d'alerte* ». Les éléments relatifs aux personnes recherchées ou signalées sont-ils issus des traitements précités ? En outre, concernant les personnes faisant l'objet d'un placement, par qui et dans quelles conditions est effectuée la prise de photographies ? Quelles sont les caractéristiques techniques d'une photo permettant de recourir à un dispositif de reconnaissance faciale ? Si ces caractéristiques (dont l'objectif est d'éviter un fort taux de faux positifs) ne sont pas réunies, les personnes sont-elles quand même placées sur la liste ou pas ?

Il est à noter que le projet de Loi est silencieux quant à l'érection de la liste d'alerte en tant que traitement, ne fixe pas son contenu (nom, prénom, photos ?), et renvoie à un Arrêté Ministériel pour déterminer « *selon le motif de l'inscription, la durée de l'inscription des personnes recherchées ou signalées de la liste d'alerte* ». L'APDP s'interroge dès lors sur l'effectivité d'un suivi par la DSP de ces informations dont certaines dépendent de l'Autorité judiciaire, eu égard au risque d'un suivi permanent des personnes en situation de handicap mental.

La CCIN avait également appelé à la plus grande vigilance sur la constitution de la base de photos des personnes recherchées ou signalées. Si la DSP ne dispose pas d'une photo exploitable d'une personne dont elle détient le nom et le prénom, elle ne devrait pas pouvoir rechercher cette personne sur les réseaux sociaux ou toute autre source disponible sur Internet, avec les risques d'erreurs que cela peut représenter pour les personnes, ni permettre le détournement de finalité d'autres traitements de la DSP.

Dans les cas de flagrance, qui relèvent de l'autorité du Procureur Général en application du Livre préliminaire du Code de Procédure Pénale, l'APDP s'interroge à la fois sur les modalités de collecte de la photo de la personne suspectée à des fins de recherche, de son insertion au sein de la liste d'alerte, et du régime d'identification biométrique à distance en jeu, c'est-à-dire en temps réel ou *a posteriori*.

En outre, comment sont gérés les cas des personnes devant sortir ou entrer dans la liste au gré des événements sportifs desquels elles sont interdites, ou des déplacements de la Famille Princièrè, pour assurer Sa protection ? Les informations proviennent-elles d'un traitement monégasque sans base légale ou d'une communication d'information de la France ou d'instances européennes ?

En ce qui concerne la volonté affichée de rechercher les personnes listées par INTERPOL, l'APDP constate qu'a été rajouté depuis la saisine de la CCIN sur le présent projet, l'alinéa suivant à l'article 8-3 :

« Dans les mêmes conditions, il peut également procéder à l'inscription, sur ces listes, des personnes signalées ou recherchées à l'étranger pour l'un ou plusieurs des motifs visés aux points 1 à 5 du premier alinéa, lorsque ces personnes font l'objet d'une notice, d'une fiche ou d'une information diffusée ou échangée sur le fondement des traités et accords internationaux auxquels la Principauté est partie, ou dans le cadre des organisations internationales de police ou de sécurité dont elle est membre ».

A titre liminaire, l'APDP s'interroge sur la faculté de la DSP, tant légalement que techniquement, d'insérer au sein de son logiciel d'identification biométrique à distance l'ensemble des photos de personnes faisant l'objet de notice d'INTERPOL, ou de tout autre organisme « étranger » ainsi que, le cas échéant, sur sa faculté à suivre l'évolution desdites notices pour supprimer les personnes concernées de la liste d'alerte, si une telle utilisation est prévue.

Elle relève en outre que l'inscription est discrétionnaire (peut également procéder), sans que l'on sache quels seront les critères choisis pour insérer une personne dans une liste d'alerte monégasque.

De plus, l'APDP n'est pas en capacité de savoir si les photos fournies par des tiers ont une qualité d'image nécessaire pour ne pas faire augmenter le risque de faux positifs. A titre d'exemple, les notices jaunes présentes sur le site d'INTERPOL ne sont clairement pas d'une qualité suffisante pour être utilisées de manière fiable dans un système de reconnaissance faciale.

Cette question de la qualité minimum des images, quelle que soit la source de ces dernières, et de leur éventuel contrôle par la DSP préalablement à leur soumission à l'outil d'identification biométrique, n'est pas documentée dans le projet de Loi, et devrait l'être au sein d'une analyse d'impact.

Enfin, concernant les notices jaunes qui selon le site d'INTERPOL « sont émises en vue de la localisation de personnes disparues, souvent mineures, ou de l'identification de personnes dans l'incapacité de s'identifier elles-mêmes », les personnes concernées sont appelées à figurer dans la « liste d'alerte portant sur les personnes recherchées ou signalées au titre d'enquêtes diligentées dans le cadre de recherches des causes de la mort, de personnes disparues, de disparitions inquiétantes ou de fugues de mineurs ». Or, ce domaine n'est pas réglementé en Principauté et l'APDP s'interroge donc sur les modalités de constitution de cette liste.

C) Sur les mises à dispositions des images de vidéosurveillance et vidéoprotection à la Direction de la Sûreté Publique

Comme indiqué supra, il est prévu que l'article 5 de la Loi n° 1.430 soit modifié pour indiquer que « les images des systèmes de vidéoprotection mis en œuvre par toute autorité administrative autre que la Direction de la Sûreté Publique, peuvent être mises à disposition de ladite Direction au moyen des équipements et liens techniques destinés à y pourvoir dans les conditions prévues par arrêté ministériel », et d'introduire au sein de cette dernière un article 5 bis qui prévoit que « Les images des systèmes de vidéosurveillance, autorisés par le Ministre d'État, installés dans les lieux ouverts au public ou filmant les abords de voies publiques, d'espaces ouverts au public ou à la circulation du public, sont mises à disposition ».

de la Direction de la Sûreté Publique au moyen des équipements et liens techniques destinés à y pourvoir dans les conditions prévues par arrêté ministériel ».

A titre liminaire, il convient de relever que la mise à disposition au moyen d'équipements et lien technique semble s'analyser comme une interconnexion permettant à la DSP *a minima* de récupérer directement le flux vidéo des entités concernées.

En outre, il est également à noter la différence de sémantique entre les images de vidéoprotection qui peuvent être mises à disposition et celles de vidéosurveillance qui sont mises à disposition. Cette différence pourrait avoir de l'importance car en l'absence de cas d'usage anticipable (exemple, utilisation uniquement en cas de menace avérée d'un individu préalablement identifié), il n'est pas possible de savoir ce qui justifie le recours à la mise à disposition, ni d'être certain que cette mise à disposition soit limitée dans le temps. Aussi, en appliquant l'article 5 bis de manière extensive, il est possible pour la DSP de capter de manière permanente le flux de vidéosurveillance d'entités, augmentant de manière pérenne le réseau de caméras qu'elle exploite, et étendant, sans que le public ne le sache, l'utilisation de l'identification biométrique à distance dans de nombreux lieux ouverts au public, tels que des halls d'hôtels, des restaurants,

A titre d'exemple, alors même qu'il n'est pas possible pour les forces intérieures françaises de mettre en œuvre un système d'identification biométrique à distance, le Code de Sécurité Intérieure français pose des limites quant à leur accès à des images de vidéoprotection.

D) Sur la modification de l'article 5 de la Loi n° 1.430

L'APDP constate que l'insertion d'un 10° après le chiffre 9° du premier alinéa de l'article 5 permet « *la détection, la recherche et l'identification des personnes recherchées ou signalées conformément aux dispositions du Titre VI bis* ».

Elle souligne qu'aux termes du Titre VI bis susvisé, est interdit pour toute autre personne que la DSP d'utiliser un « *système d'identification biométrique à distance aux fins de rechercher ou d'identifier les personnes physiques* ». Elle note ainsi que la notion de détection présente au 10° projeté disparaît de l'interdiction formulée dans le projet d'article 8-1.

Le Titre VI bis prévoyant que l'identification biométrique à distance ne peut être mise en œuvre que par la DSP, l'APDP s'interroge donc quant à la pertinence d'insérer ce 10° à l'article 5 qui concerne les Autorités administratives compétentes, pouvant laisser croire à une utilisation plus large, notamment à des fins de détection. Ce sentiment est même renforcé par le nom du projet de Loi « *relative à l'utilisation de la vidéoprotection et de la vidéosurveillance des lieux accessibles au public pour la détection, la recherche et l'identification des personnes recherchées ou signalées au moyen de système d'identification biométrique à distance* », qui laisse à penser que tout système de vidéosurveillance peut être doté d'un système de reconnaissance faciale, quel que soit le responsable de traitement.

L'APDP s'interroge même sur la possibilité pour toute autre Autorité publique compétente de mettre en œuvre ne serait-ce qu'un système de vidéoprotection quand l'article 1er de l'Arrêté Ministériel n° 2017-576 du 19 juillet 2017 portant application de l'article 5 de la Loi n° 1.430 du 13 juillet 2016 portant diverses mesures relatives à la préservation de la sécurité nationale dispose que « *La demande d'autorisation mentionnée au quatrième alinéa de l'article 5 de la loi n° 1.430 du 13 juillet 2016, susvisée, formée auprès du Ministre d'État par le Directeur de la Sûreté Publique, porte sur un ensemble de caméras ou de dispositifs de vidéoprotection situés dans une même zone géographique, dans la limite des quartiers ordonnancés définis par l'Ordonnance Souveraine n° 3.647 du 9 septembre 1966 concernant*

l'urbanisme, la construction et la voirie. (...) ». Dès lors, seule la DSP peut solliciter l'installation d'un système de vidéoprotection.

En tout état de cause, l'APDP estime qu'il ne devrait pas y avoir de doute, et donc d'insécurité juridique, quant à l'impossibilité pour une Autorité administrative compétente autre que la DSP de mettre en œuvre une identification biométrique à distance à des fins de détection.

E) Sur le projet d'article 8-6 de la Loi n° 1.430

Le projet d'article 8-6 dispose que *« Les données qui ont donné lieu à un rapprochement positif par le système (...) sont conservées trente jours à compter du jour de ce rapprochement positif, sauf si leur conservation, au-delà de cette durée, est nécessaire :*

- 1. aux enquêtes judiciaires concernant une infraction punie d'une peine supérieure ou égale à un an d'emprisonnement ;*
- 2. à la poursuite des finalités énoncées au deuxième alinéa de l'article 9 de la loi n° 1.430 du 13 juillet 2016 ».*

L'APDP ne comprend pas de quelles *« données »* il s'agit. L'exposé des motifs indique que cet article a vocation *« à encadrer les conditions de l'archivage des rapprochements positifs »*, ce qui n'apporte pas de précision quant à leur nature. Parle-t-on des images de vidéoprotection, qui ont déjà une durée de conservation de trente jours, ou d'éléments en lien avec le système d'identification biométrique à distance, telle qu'une surcouche logicielle sur les images vidéo pour individualiser une personne dans la foule sur un film, ou encore l'affichage du taux de confiance de l'Intelligence Artificielle quant à la similarité entre la personne à rechercher et celle identifiée ?

Si ces éléments doivent être considérés comme des pièces de l'enquête judiciaire, ils relèvent des dispositions du Code de Procédure Pénale et mériteraient peut-être un encadrement particulier en son sein.

Concernant la conservation des informations pour *« la poursuite des finalités énoncées au deuxième alinéa de l'article 9 de la Loi n° 1.430 »*, l'APDP s'inquiète que l'identification biométrique à distance serve de technique de renseignement qui échapperait, elle, à tout contrôle de la Commission Spéciale de Sécurité Nationale et au recours à au juge.

En outre, l'exposé des motifs indiquant que ces personnes ont vocation à être suivies et non arrêtées, le rapprochement positif les concernant peut être continu dans le temps. Les vidéos alimentent-elles en continu un traitement de renseignement ?

En tout état de cause, l'APDP estime qu'en cas d'adoption en Principauté d'une telle technologie, et sous le contrôle d'un organisme indépendant, il devrait être dressé un bilan précis des rapprochements positifs par le système mais aussi des faux positifs constatés, avant et après intervention d'un opérateur de la DSP, et, le cas échéant, de la raison ayant conduit l'Intelligence Artificielle à se tromper, afin de maintenir une exigence continue de conformité de la solution choisie. La publication d'un rapport public annuel de l'utilisation de cette technologie, et de ses statistiques, devrait, à des fins de transparence, être également prévue dans le projet de Loi.

F) Sur le projet d'article 8-7 de la Loi n° 1.430

L'article 8-7 projeté dispose que *« Les données traitées dans le cadre des opérations visées à l'article 8-2 ne peuvent faire l'objet d'aucune interconnexion avec d'autres données personnelles ou fichiers contenant des données personnelles ».*

L'APDP s'interroge, comme au point précédent, sur la nature des données en jeu : s'agit-il des images vidéo, des éléments propres à une surcouche logicielle, des informations contenues dans la liste d'alerte, ou de tous ces éléments à la fois ?

L'exposé des motifs indique qu'« *Enfin, l'article 8-7 précise que l'identification des personnes qui sera faite par le logiciel d'analyse d'images sera exclusivement limitée au traitement des données des personnes inscrites sur la liste d'alerte, et ne fera naturellement l'objet d'aucune interconnexion avec d'autres traitements de données personnelles mis en œuvre par la Direction de la Sûreté Publique.*

En particulier, aucune « recherche » ou « identification » aléatoire ne pourra être réalisée dans la mesure où la comparaison sera opérée sur la base objective des personnes figurant dans la liste d'alerte, laquelle fonctionnera selon les conditions d'inscription, de mise à jour et d'effacement strictement définies par la loi et l'arrêté ministériel d'application de celle-ci ».

L'APDP relève toutefois que les modalités de création de la liste ne sont pas précisées, et l'Arrêté Ministériel d'application est limité par sa rédaction dans sa portée. Il est difficile, en l'état du texte projeté et des propos tenus par les représentants des Autorités, d'imaginer que cette « *liste d'alerte* », pour sa constitution, soit autonome, de traitements tiers, dont elle suppose l'existence, tels que le « *Fichier des personnes recherchées ou signalées* », voire des fichiers d'interdits de stade exploités par des entités étrangères, ou encore les clichés d'INTERPOL.

En outre, en application de l'article 8-6 projeté, les « *données* » dont s'agit alimentent les traitements de police judiciaire et de renseignement. Dès lors, si les données ne sont peut-être pas interconnectées au sens de la protection des données, c'est-à-dire transmises directement par un lien technique, elles semblent du moins rapprochées avec d'autres traitements.

G) Un texte « *chapeau* », inadapté et lacunaire

Le projet de Loi n° 1087 s'inspire en partie des notions du Règlement européen dit de l'AI ACT, qui, bien que s'agissant d'un Règlement d'application directe au sein de l'UE, fait effet de « *texte chapeau* » pour l'encadrement des systèmes d'identification biométrique à distance à des fins répressives. Ce Règlement renvoie en effet à un nécessaire encadrement au sein des Lois des pays désirant mettre en œuvre un tel système. Le texte monégasque ne peut donc se contenter des dispositions projetées, très lacunaires, pour encadrer un sujet aussi sensible. Aucun des textes en projet étudiés par l'APDP ne va aussi loin que la Loi monégasque avec aussi peu de garanties associées.

En outre, le projet de Loi mélange toutes les notions sans jamais les définir, parlant pêle-mêle d'identification biométrique à distance en temps réel et *a posteriori*, pour des missions de police judiciaire mais aussi administrative, centré sur le système de vidéoprotection de la DSP mais ouvert à d'autres vidéoprotection et vidéosurveillance.

In fine, le texte projeté ne semble avoir pour seul objectif qu'offrir une base légale à la mise en œuvre, *a minima*, d'un système de reconnaissance faciale, dont la seule garantie réelle est la confiance que l'on doit accorder à son utilisation, sans contrôle externe effectif, ni lors de l'élaboration et de la tenue des listes, ni lors de l'utilisation de la technologie. Aucune justification de la nécessité absolue de sa mise en œuvre n'est avancée. Aucun cas d'usage n'est mis en exergue. Rien ne vient justifier la nécessité et la proportionnalité du dispositif, notamment pourquoi le système doit être permanent et non déployé seulement en cas de besoin, selon un principe de subsidiarité, c'est-à-dire uniquement si une solution moins attentatoire que la biométrie est impossible dans un cas d'espèce.

Au contraire, l'imprécision du texte pose de nombreux problèmes de fond quant au respect des droits et libertés fondamentaux des personnes concernées et il est aisé d'imaginer des situations d'utilisation légale mais trop extensive du dispositif, permettant un contrôle continu de la vie privée de personnes identifiées dans la sphère publique. En effet, le fait que le projet permette d'identifier des personnes signalées, et donc des personnes qui ne doivent pas nécessairement faire l'objet d'une interpellation, permet à la DSP de suivre les personnes tant qu'elles n'ont pas été retirées d'une liste d'alerte. S'ensuit ainsi un potentiel contrôle continu des déplacements, des interactions, des habitudes de vie d'une personne.

De plus, les interactions avec les techniques de renseignement – et les traitements qu'elles alimentent, sont floues et échappent à tout contrôle.

A cela s'ajoute le fait que l'utilisation détournée de l'identification biométrique à distance est plus faiblement sanctionnée dans le projet de Loi n° 1087 qu'en application de la Loi n° 1.565, et une utilisation abusive et détournée par un personnel de la DSP n'est assortie d'aucune sanction dans ledit projet.

L'APDP estime également que contrôler la qualité et la proportionnalité de l'utilisation d'un tel dispositif apparaît techniquement compliqué, et que les cas d'utilisation extensive peuvent être difficiles à mettre en exergue.

Il convient également de constater qu'« *Un arrêté ministériel détermine les éléments d'identification de ces personnes et, pour chacune des listes visées au premier alinéa, la durée de leur inscription sur celles-ci.*

Cette durée est fixée en considération du motif pour lequel la liste dont s'agit est établie. Les personnes concernées sont radiées des listes d'alerte sur lesquelles elles sont inscrites, avant l'écoulement de cette durée, soit que le motif de leur inscription n'est plus établi, soit que la finalité poursuivie par leur inscription est atteinte ».

L'encadrement des listes d'alerte est donc géré par voie réglementaire, tant pour l'établissement de la durée de conservation de chaque liste que pour l'appréciation de la raison de l'inscription sur ladite liste des personnes concernées.

Par ailleurs, l'APDP estime qu'il aurait été intéressant de réfléchir à un droit à réparation pour les personnes qui seraient victimes d'un préjudice, telle qu'une garde à vue induite, sur la base d'une erreur logicielle non détectée par un agent superviseur de la DSP, et de manière plus large à un système de responsabilité, que ce soit de la DSP et de ses agents en tant que responsable de traitement, que du prestataire à l'origine de l'IA utilisée.

De plus, l'identification biométrique à distance étant interconnectée à des systèmes de vidéoprotection et de vidéosurveillance extérieurs à la DSP, vraisemblablement sur le système d'information de cette dernière, l'Autorité s'interroge sur les éventuelles responsabilités en cas de défaut de sécurité de ces systèmes tiers, ou de fuites d'images vidéo en lien avec des enquêtes.

Tel est l'avis de l'Autorité de Protection des Données Personnelles

Le Président

Robert CHANAS