

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 l'identification des personnes recherchées ou signalées au moyen d'identification biométrique à distance.

Avis du Haut Commissariat à la Protection des Droits, des Libertés et à la Médiation

Par courrier en date du 8 octobre 2025, le Conseil National a saisi le Haut Commissariat pour avis sur 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 d'identification biométrique à distance.

Cette réforme est présentée comme une démarche de modernisation de l'arsenal juridique de l'Etat en vue de répondre aux exigences contemporaines de la lutte contre la délinquance tout en s'assurant de la protection des intérêts fondamentaux de la Principauté.

Ce projet est en cohérence avec les récentes avancées européennes, à savoir le Règlement de l'Union Européenne sur l'intelligence artificielle, entré en vigueur en août 2024 et la Convention cadre du Conseil de l'Europe sur l'intelligence artificielle, ouverte à la signature depuis septembre 2024.

Le Haut Commissariat salue donc cette initiative car il estime indispensable que des dispositions légales viennent encadrer cette matière particulièrement sensible qui touche aux droits fondamentaux et dont le traitement est un marqueur en ce qui concerne le respect de l'Etat de Droit, à l'heure où les dispositifs faisant intervenir l'intelligence artificielle se développent à un rythme exponentiel.

Il apparaît également au Haut Commissariat que le guide de la Principauté dans l'élaboration de cette législation devrait être le respect et l'application effective des principes posés par sa Constitution et par ses engagements internationaux en matière de Droits de l'Homme.

Aussi, dans son étude, le Haut Commissariat a-t-il en premier lieu tenté de mieux cerner le contexte et les enjeux de l'utilisation d'applications de reconnaissance faciale, plus particulièrement en matière de sécurité publique, afin de déterminer les principes de droit qui doivent s'y appliquer.

En second lieu, le Haut Commissariat a procédé à l'analyse des dispositions de la loi à la lumière des principes précités ce qui l'a conduit à constater, qu'en l'état, ces dernières paraissent insuffisantes pour garantir sans ambiguïté aucune la protection des droits des personnes concernées.

I- DEFINITION ET ENJEUX DES TECHNOLOGIES DE RECONNAISSANCE BIOMETRIQUE A DISTANCE

1°/ Définition :

Le Haut Commissariat a dans un premier temps souhaité mieux cerner le champ couvert par le terme d'*« utilisation de la vidéoprotection et de la vidéosurveillance des lieux accessibles au public pour la détection, la recherche l'identification des personnes recherchées ou signalées au moyen d'identification biométrique à distance »* en identifiant les techniques et notamment les applications logicielles qu'appellent la mise en œuvre de ce dispositif.

Il s'avère que la mise en œuvre d'un tel système implique l'utilisation de logiciels de reconnaissance faciale, qu'il importe de définir :

Un système de reconnaissance faciale est une application logicielle visant à reconnaître une personne grâce à son visage de manière automatique.

La reconnaissance de visages a de nombreuses applications en vidéosurveillance, biométrie, robotique, indexation d'images et de vidéos, recherche d'images par le contenu, etc. Ces systèmes sont généralement utilisés à des fins de sécurité pour déverrouiller ordinateur/mobile/console, mais aussi en domotique. Le fonctionnement de ces systèmes se base sur une ou plusieurs caméras pour reconnaître l'utilisateur.

Ils peuvent également être utilisés, normalement avec le consentement de l'utilisateur, pour lui faciliter l'usage de certains réseaux sociaux ou applications (Facebook, Google...)

Les deux types de tâches effectuées par ces systèmes sont :

- L'identification qui consiste à déterminer l'identité d'un individu parmi N identités connues, présentes dans une base.
- La vérification, laquelle consiste à s'assurer que l'identité prétendue est bien la bonne.

La sécurité est le principal domaine d'application des systèmes de reconnaissance faciale, et l'un des domaines importants d'application de ces systèmes est la surveillance facilitant la recherche de l'identité d'une personne à l'aide d'une photo ou d'une vidéo.

Des systèmes de reconnaissance faciale ont ainsi été construits autour du déploiement de caméras de vidéosurveillance connectées à un réseau de télécommunication et à des applications d'intelligence artificielle. A partir de ces technologies s'est défini le concept de ville sûre, extension de la ville intelligente.

Des exemples en sont le système de reconnaissance faciale développé actuellement aux Etats Unis par le FBI appelé NGIS (Next Generation Identification System), ou celui actuellement utilisé par la NSA qui se base entre autres sur les images postées sur les réseaux sociaux.

2°/ L'utilisation de ce type de technologie met toutefois en tension l'équilibre entre liberté et sécurité :

Dans plusieurs Etats européens, l'utilisation de ces systèmes a déjà suscité des difficultés juridiques importantes.

L'usage du logiciel CLEAR VIEW AI (une entreprise américaine qui a développé un outil de reconnaissance faciale universel), qui permet de comparer une photographie avec une base de données de plus de trois milliards de photographies initialement publiées sur internet, était légalement utilisé par plus de 600 bureaux de police nord-américains en février 2020 et par certains Etats européens.

Toutefois, plusieurs de ces administrations européennes ont ensuite été condamnées par leur propres juridictions et autorités pour l'utilisation de ce logiciel en application des lois relatives à la protection des données personnelles. Ainsi la police suédoise a été condamnée par l'autorité suédoise de protection des données personnelles à une amende de 250 000 euros.

En France, la CNIL a mis en demeure la société CLEAR VIEW AI de cesser sa réutilisation de photographies accessibles sur internet puis l'a condamnée à une amende de 20 millions d'euros. Le 13 avril 2023, la CNIL a décidé de liquider l'astreinte prononcée à l'encontre de CLEARVIEW AI. La société devait payer la somme de 5 200 000 euros pour ne pas s'être conformée à l'injonction formulée dans la décision de sanction d'octobre 2022.

Par ailleurs, la Cour d'Appel de Londres a pris en 2020 une décision concluant que les services de police ne s'étaient pas suffisamment assurés de l'absence de biais discriminatoires du logiciel utilisé quant à l'origine ethnique ou au genre des personnes qu'il visait à identifier, les risques de discrimination découlant de l'utilisation même des outils biométriques (Court of Appeal R (bridges) v. Chief Constable of South Wales Police 2019, EWHC 2341 (Admin)).

Ainsi, la question du cadre légal de l'utilisation de ces systèmes se pose dans tous les pays européens et des normes internationales spécifiques ont été récemment adoptées afin de définir les principes devant s'appliquer afin de garantir la protection des droits.

II – LE CADRE LEGAL

1°/ En droit interne monégasque :

L'article 22 de la Constitution de la Principauté de Monaco prévoit que toute personne a droit au respect de sa vie privée.

L'article 1^{er} de la loi n° 1.565 du 3 décembre 2024 relative à la protection des données personnelles prévoit que *« les traitements automatisés ou non automatisés de données à caractère personnel ne doivent pas porter atteinte aux libertés et droits fondamentaux consacrés par le titre III de la Constitution. Les droits des personnes physiques concernées par ces traitements sont garantis par la présente loi et s'exercent selon les modalités qu'elle définit. »*

Cette même loi prévoit en outre dans son Titre VI des dispositions particulières concernant les données sensibles et notamment les traitements mis en œuvre par les autorités chargées de la prévention, de la détection, des poursuites et de la répression des infractions pénales et de la protection de l'ordre public et de la sécurité nationale.

2°/ En droit européen :

➤ En ce qui concerne le Conseil de l'Europe :

En premier lieu, la Convention Européenne des Droits de l'Homme, en son article 8, instaure le droit au respect de la vie privée en ce compris le droit à l'image et à la protection des photographies. Cet article, d'application directe à Monaco, prévoit ainsi :

« 1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.

2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui ».

Selon une jurisprudence constante, la Cour Européenne des Droits de l'Homme considère ainsi que la mémorisation ou l'utilisation des données personnelles, ou même leur communication, constitue une ingérence dans l'exercice du droit au respect de la vie privée et familiale consacré par l'article 8-1 de la CEDH.

Concernant plus particulièrement l'emploi des techniques de reconnaissance faciale, l'arrêt *Glukhin c/ Russie*, rendu en 2023, a porté sur l'utilisation par la police russe de techniques de reconnaissance faciale dans la poursuite d'une infraction administrative. Dans cette affaire, la Cour a notamment précisé que, même si un texte de niveau réglementaire prévoyait cette possibilité dans le cas d'espèce, *« les mesures en question étaient particulièrement intrusives, surtout celles qui faisaient appel à une technologie de reconnaissance faciale à la volée. Le niveau de justification exigé pour qu'elles puissent passer pour « nécessaires dans une société démocratique » est donc élevé, et le recours à une technologie de reconnaissance faciale à la volée requiert pour sa part le niveau de justification le plus élevé »* à savoir un *« besoin social impérieux »*.

D'autre part, la Convention 108 + pour la Protection des personnes à l'égard du traitement des données à caractère personnel, à laquelle Monaco est partie, dispose en son Article 1 que : *« le but de la présente Convention est de garantir, sur le territoire de chaque Partie, à toute personne physique, quelles que soient sa nationalité ou sa résidence, le respect de ses droits et de ses libertés fondamentales, et notamment de son droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant »*.

Les lignes directrices d'application de ladite Convention prévoient également que *« si elles envisagent le déploiement des technologies de reconnaissance faciale dans les environnements non contrôlés (c'est-à-dire ouverts au public), les autorités chargées de l'application de la loi devront :*

- *Evaluer 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 »*

Le Comité consultatif de cette convention a également émis des lignes directrices sur la reconnaissance faciale qui contiennent notamment des orientations à l'intention des entités utilisant des technologies de reconnaissance faciale. En 2021, ces lignes directrices ont notamment précisé que *« l'intégration de technologies de reconnaissance faciale dans les systèmes de surveillance existants fait courir des risques sérieux aux droits au respect de la vie privée et à la protection des données à caractère personnel, ainsi qu'à d'autres droits fondamentaux puisque leur utilisation n'impose pas toujours que les personnes dont les données biométriques sont ainsi traitées en soient informées ou y coopèrent. C'est le cas par exemple avec la possibilité d'accéder à des images numériques de personnes sur internet.*

Afin de prévenir de telles atteintes, les Parties à la Convention 108+ s'assureront que le développement et l'utilisation de la reconnaissance faciale respectent le droit à la vie privée et le droit à la protection des données personnelles, renforçant ainsi les droits de l'homme et les libertés fondamentales par la mise en œuvre des principes consacrés par la convention dans le contexte particulier des technologies de reconnaissance faciale ».

Enfin, la nouvelle Convention-cadre du Conseil de l'Europe relative à l'intelligence artificielle, déjà adoptée par 18 pays ou organisation (dont l'UE, la Suisse, Andorre, Saint Marin, le Liechtenstein), établit les principes fondamentaux suivants applicables aux activités menées dans le cadre du cycle de vie des systèmes d'IA :

- Dignité humaine et autonomie personnelle ;
- Egalité et non-discrimination ;
- Respect de la vie privée et protection des données à caractère personnel ;
- Transparence et contrôle ;
- Obligation de rendre des comptes et responsabilité ;
- Fiabilité ;
- Innovation sûre.

Ce texte prévoit également les recours, droits procéduraux et garanties suivants :

- Documenter les informations pertinentes concernant les systèmes d'IA et leur utilisation, et les mettre à la disposition des personnes concernées ;
- Les informations doivent être suffisantes pour permettre aux personnes concernées de contester la ou les décisions prises par le biais de l'utilisation du système ou fondées en grande partie sur celui-ci, et de contester l'utilisation du système lui-même ;
- Possibilité effective de former un recours auprès des autorités compétentes ;
- Mise à disposition des personnes affectées de garanties, de protections et de droits procéduraux effectifs lorsqu'un système d'intelligence artificielle a un impact significatif sur la jouissance des droits humains et des libertés fondamentales ;
- Notification aux personnes concernées du fait qu'elles interagissent avec des systèmes d'intelligence artificielle et non avec un humain.

Enfin, le texte fixe des exigences en matière de gestion des risques et des impacts :

- Conduite d'évaluations des risques et des impacts, qu'ils soient réels ou potentiels sur les droits humains, la démocratie et l'État de droit, menées de manière itérative ;
- Mise en place des mesures de prévention et d'atténuation suffisantes résultant de la mise en œuvre de ces évaluations ;
- Possibilité pour les autorités d'instaurer un moratoire ou une interdiction pour certaines utilisations de systèmes d'IA (« lignes rouges »).

➤ En ce qui concerne le droit communautaire :

Le cadre juridique applicable est le droit commun de la protection des données personnelles à savoir :

- Le Règlement (UE)2016/679 du 27 avril 2016 (RGPD) ;
- La Directive (UE) 2016/680 du 27 avril 2016 (Police-Justice).

Il est aussi possible de se référer aux lignes 05/2022 directrices du Comité Européen pour la protection des données en matière d'usage de la reconnaissance faciale en matière répressive qui expose notamment des scénarios concrets d'usage de ces techniques par les forces de l'ordre illustrant la mise en œuvre des principes de la convention 108 + et du RGPD.

Par ailleurs, l'UE a adopté en août 2024 un Règlement européen établissant des règles harmonisées concernant l'intelligence artificielle dont les objectifs spécifiques sont notamment les suivants :

- « veiller à ce que les systèmes d'IA mis sur le marché de l'Union et utilisés soient sûrs et respectent la législation en vigueur en matière de droits fondamentaux et les valeurs de l'Union;
- renforcer la gouvernance et l'application effective de la législation existante en matière de droits fondamentaux et des exigences de sécurité applicables aux systèmes d'IA ».

Le Haut Commissariat a recensé les principes essentiels posés par les textes précités concernant l'usage de la reconnaissance faciale :

L'utilisation de systèmes de reconnaissance faciale est considérée comme a priori contraire au respect de la vie privée et les risques encourus de préjudices à d'autres types de liberté et d'amplification des discriminations sont également soulignés par les instances du Conseil de l'Europe et de l'Union européenne, ainsi que par le Défenseur des Droits français.

Ainsi, ces textes prévoient la mise en œuvre de tels systèmes de manière extrêmement restrictive et uniquement dans le respect des principes suivants :

Protection des Droits et libertés fondamentaux

Les droits à la vie privée, à la liberté d'expression, à la liberté de réunion, le droit d'aller et venir, le droit à la liberté de pensée et d'opinion ne doivent pas être remis en cause par la mise en place d'un système de reconnaissance faciale. Une nouvelle notion de « *sujet d'intelligence artificielle* » dont les droits pourraient être impactés émerge en droit européen (cf. la nouvelle convention cadre du Conseil de l'Europe précitée).

Nécessité absolue

La mise en place de la reconnaissance faciale ne doit intervenir qu'en cas de nécessité absolue, par exemple en cas de menaces terroristes.

Exigence de prévisibilité

La Cour Européenne des Droits de l'Homme a exprimé dans sa jurisprudence une exigence de prévisibilité pour tout traitement d'information nominative mis en œuvre par l'autorité publique (cf. le guide sur l'article 8 de la CEDH qui garantit notamment le respect de la vie privée).

Proportionnalité

Les mesures adoptées doivent être proportionnelles au but poursuivi. L'exigence de mise en œuvre de ce principe commence à être illustré par des jurisprudences nationales, tel le jugement de la Haute Cour de Cardiff au Royaume Uni - Court of Appeal R (bridges) v. Chief Constable of South Wales Police 2019, EWHC 2341 (Admin).

Garanties appropriées des systèmes mis en œuvre/ principe de sûreté

La mise en place de garanties en matière de sûreté, de sécurité, de qualité des données, de cybersécurité et de robustesse en ce qui concerne la conception, le développement et l'application des systèmes d'intelligence artificielle est requise.

De plus, les conditions d'intervention d'un prestataire extérieur doivent être prévues par la loi.

Les autorités devraient également donner aux fournisseurs et utilisateurs de systèmes d'IA une orientation effective sur la manière d'identifier, d'évaluer, de prévenir et d'atténuer les risques et les impacts négatifs résultant de leur mise en œuvre.

Une formation appropriée des fournisseurs et des utilisateurs de ces systèmes devrait également être prévue, de même que la possibilité d'imposer un moratoire ou une interdiction à l'égard de certaines applications de systèmes d'IA.

Principe de non-discrimination

Aucune discrimination ne doit résulter de la mise en place de telles mesures qui ne doivent pas non plus risquer d'aggraver des discriminations existantes.

Transparence

Les individus doivent être informés des traitements mis en œuvre par la police utilisant ce type de système et avoir un accès direct à leurs informations.

Une autorité nationale compétente doit procéder à une évaluation approfondie de la nécessité, de la proportionnalité et des risques et impacts potentiels avant et pendant l'application d'un système d'intelligence artificielle.

Recours effectif

Une possibilité de contestation effective de l'application du système ou des décisions affectant les droits et les libertés prises à la suite de son utilisation doit être offerte, notamment pour les personnes handicapées.

Les modalités de mise en œuvre de ces principes se trouvent détaillées dans le Règlement européen sur l'intelligence artificielle et dans la Convention cadre européenne sur l'intelligence artificielle, les Droits de l'Homme, la Démocratie et l'Etat de Droit.

3°/ L'exemple de la France :

Dans le pays voisin, également partie à la Convention 108+ et soumis au RGPD, il n'existe pour l'heure aucun texte spécifique à l'utilisation de dispositifs de reconnaissance faciale.

La loi relative aux Jeux Olympiques et Paralympiques de 2024 adoptée le 19 mai 2023 qui autorisait les traitements algorithmiques d'images de vidéoprotection ou de vidéosurveillance seulement à l'occasion de cet événement. La loi olympique votée par la France prévoyait qu'une expérimentation serait utilisée uniquement à l'occasion de manifestations sportives de grande ampleur ou s'il y avait risque de terrorisme et d'atteinte grave aux personnes. Cette loi était valable de sa promulgation jusqu'en décembre 2024. C'est donc la voie de l'expérimentation, sous le contrôle de la CNIL, qui a été retenue.

Le Haut Commissariat relève toutefois que l'article 10 de cette loi autorisait uniquement les traitements algorithmiques d'images de vidéoprotection ou de vidéosurveillance strictement définis à son premier point :

« I. - A titre expérimental et jusqu'au 31 mars 2025, à la seule fin d'assurer la sécurité de manifestations sportives, récréatives ou culturelles qui, par l'ampleur de leur fréquentation ou par leurs circonstances, sont particulièrement exposées à des risques d'actes de terrorisme ou d'atteintes graves à la sécurité des personnes, les images collectées au moyen de systèmes de vidéoprotection autorisés sur le fondement de l'article L. 252-1 du code de la sécurité intérieure ou au moyen de caméras installées sur des aéronefs autorisés sur le fondement du chapitre II du titre IV du livre II du même code, dans les lieux accueillant ces manifestations et à leurs abords ainsi que dans les véhicules et les emprises de transport public et sur les voies les desservant, peuvent faire l'objet de traitements algorithmiques. Ces traitements ont pour unique objet de détecter, en temps réel, des événements prédéterminés susceptibles de présenter ou de révéler ces risques et de les signaler en vue de la mise en œuvre des mesures nécessaires par les services de la police nationale et de la gendarmerie nationale, les services d'incendie et de secours, les services de police municipale et les services internes de sécurité de la SNCF et de la Régie autonome des transports parisiens dans le cadre de leurs missions respectives ».

Il était de plus expressément prévu une information du public à son point III : « ...III. - Le public est préalablement informé, par tout moyen approprié, de l'emploi de traitements algorithmiques sur les images collectées au moyen de systèmes de vidéoprotection autorisés sur le fondement de l'article L. 252-1 du code de la sécurité intérieure et de caméras installées sur des aéronefs autorisés sur le fondement du chapitre II du titre IV du livre II du même code, sauf lorsque les circonstances l'interdisent ou que cette information entrerait en contradiction avec les objectifs poursuivis. Une information générale du public sur l'emploi de traitements algorithmiques sur les images collectées au moyen de systèmes de vidéoprotection et de caméras installées sur des aéronefs est organisée par le Ministre de l'Intérieur... »

Cette loi interdisait toutefois l'usage des techniques de reconnaissance faciale à son point IV : « les traitements mentionnés au I du présent article n'utilisent aucun système d'identification biométrique, ne traitent aucune donnée biométrique et ne mettent en œuvre aucune technique de reconnaissance faciale. Ils ne peuvent procéder à aucun rapprochement, à aucune interconnexion ni à aucune mise en relation automatisée avec d'autres traitements de données à caractère personnel. Ils procèdent exclusivement à un signalement d'attention, strictement limité à l'indication du ou des événements prédéterminés qu'ils ont été programmés à détecter. Ils ne produisent aucun autre résultat et ne peuvent fonder, par eux-mêmes, aucune décision individuelle ni aucun acte de poursuite ».

Par ailleurs, la commission des lois du sénat a formulé 30 propositions sur la reconnaissance faciale afin d'écarter le risque d'une société de surveillance. Elle préconisait d'autre part que, si des usages devaient être validés, l'adoption d'une loi d'expérimentation serait nécessaire « *pour créer le débat et déterminer les usages de l'expérimentation* » (...) « *elle 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* ».

Le Sénat avait 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* ».

Une proposition de loi visant à l'interdiction de la reconnaissance faciale a été déposée le 17 avril 2025 à l'Assemblée Nationale. Elle vise à interdire l'installation, l'activation ou l'utilisation de toute technologie de reconnaissance faciale à des fins d'identification d'une personne physique de manière

unique. Cette interdiction est insérée dans la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

La proposition de loi s'inscrit dans un cadre de régulation et de cadrage de l'utilisation de la reconnaissance biométrique par les pouvoirs publics. Elle définit des lignes rouges et des grands principes pour l'utilisation de la reconnaissance biométrique dans l'espace public, tels que la nécessité du consentement des personnes concernées et l'interconnexion avec d'autres données personnelles.

La proposition de loi met en garde contre la normalisation de ces technologies et souligne que les moyens humains sont plus efficaces pour la sécurité publique que les technologies de surveillance. Elle insiste sur la nécessité d'une interdiction claire pour protéger les droits humains et éviter une société de suspicion et de contrôle.

Si le texte pose des limites, il autorise aussi l'expérimentation pour une durée de trois ans de l'usage de la reconnaissance faciale dans l'espace public dans des cas justifiés par un "*intérêt public supérieur*".

La proposition de loi précise le cadre de l'expérimentation notamment l'accès par reconnaissance faciale pour :

- L'authentification biométrique sans consentement pour l'accès à certains grands événements ;
- Le traitement des données biométriques *a posteriori* dans le cadre d'enquêtes judiciaires ou en matière de renseignement ;
- Le traitement de données biométriques en temps réel pour lutter contre le terrorisme et la grande criminalité.

Ces expérimentations permettront de définir au cas par cas les utilisations des technologies de reconnaissance faciale acceptables au vu des bénéfices obtenus et des principes de nécessité, de proportionnalité.

C'est à la lumière des principes et exemples précités que le Haut Commissariat a examiné le dispositif du projet de loi.

III – ANALYSE DES DISPOSITIONS DU PROJET DE LOI

L'objet du présent projet de loi est de permettre à la Direction de la Sûreté Publique d'avoir recours à la reconnaissance faciale afin de rechercher et d'identifier des personnes figurant sur des listes d'alerte dans les lieux accessibles au public.

Ce nouveau texte se présente comme une modification de la loi n°1.430 du 13 juillet 2016, modifiée, en y ajoutant des articles nouveaux traitant notamment de la reconnaissance faciale. Il comprend quatre articles qui créeraient deux nouvelles sections au sein de la loi n°1.430.

Le Haut Commissariat rappelle au préalable qu'à l'époque du vote de cette loi, sur laquelle il n'avait pas été consulté, une menace terroriste pesait sur le pays voisin, créant une urgence particulière.

C'est dans ce contexte que cette législation avait doté la police d'outils supplémentaires afin d'assurer la sécurité et veiller au maintien de l'ordre public. Elle avait de plus redéfini les missions et les pouvoirs de la police administrative en les enrichissant et en les encadrant, notamment, en créant un mécanisme d'autorisation par le Ministre d'Etat et de contrôle de l'utilisation de certaines techniques d'enquête particulièrement intrusives en prévoyant des contrôles et des recours devant la commission créée à son article 16.

L'analyse du présent projet de loi révèle toutefois que, malgré la référence à la loi n° 1.165 du 23 décembre 1993 relative à la protection des informations nominatives (désormais abrogée et remplacée par la loi n° 1.565 du 3 décembre 2024) et l'adoption de dispositions complémentaires, le manque de clarté concernant son articulation avec les autres textes en vigueur et l'absence de certaines mesures ne lui permettent pas d'offrir toutes les garanties nécessaires au respect de la protection des droits.

1°/ Les dispositions des articles 6 et 7 de la loi 1.430 placent les traitements de reconnaissance faciale sous l'empire de la loi relative à la protection des données nominatives :

Le Titre V de la loi n°1.430 comporte des dispositions relatives aux traitements automatisés d'informations nominatives mis en œuvre par la Direction de la Sûreté Publique et renvoie dans son article 6 à la loi n° 1.165 du 23 décembre 1993 relative à la protection des informations nominatives qui dispose dans son article 1^{er} que « *les traitements automatisés ou non automatisés d'informations nominatives ne doivent pas porter atteinte aux libertés et droits fondamentaux consacrés par le titre III de la Constitution* » et notamment à l'article 22 de la Constitution garantissant le droit au respect de sa vie privée et familiale et au secret de sa correspondance.

La référence à ces droits figure également à l'article premier de la loi n° 1.565 du 3 décembre 2024 relative à la protection des données personnelles qui a remplacé le texte précité et énonce que « *les traitements automatisés ou non automatisés de données à caractère personnel ne doivent pas porter atteinte aux libertés et droits fondamentaux consacrés par le titre III de la Constitution. Les droits des personnes concernées par ces traitements sont garantis par la présente loi et s'exercent selon les modalités qu'elle définit* ».

Par ailleurs, la loi n°1.430 susvisée prévoit que « *Le Directeur de la Sûreté Publique prend toutes mesures utiles, au regard de la nature des informations nominatives figurant dans les traitements mentionnés à l'article précédent aux fins de :*

- *Préserver leur intégrité en empêchant notamment qu'elles soient déformées ou endommagées ;*
- *Veiller à ce qu'elles soient inaccessibles à des tiers non autorisés.*

Il est tenu d'en assurer la mise à jour et de veiller, selon les besoins, à ce qu'elles soient complétées, rectifiées ou effacées.

Seuls les personnels de la Direction de la Sûreté Publique dûment et spécialement habilités par le Directeur de la Sûreté Publique peuvent accéder auxdites informations.

L'habilitation précise les traitements auxquels elle autorise l'accès.

La traçabilité de l'accès aux traitements mentionnés à l'article précédent est assurée au moyen d'une journalisation périodique. Le responsable du traitement veille à la conservation des données relatives à cette journalisation pendant dix ans.

Les modalités d'application du présent article sont définies par arrêté ministériel ».

L'Article 4 du projet de loi détaille en outre les dispositions spécifiques pour le recours aux technologies d'identification biométrique à distance par les services de police à partir des images des lieux publics captés par les caméras de vidéoprotection ou vidéosurveillance :

Huit articles créent ainsi un cadre spécifique pour le recours aux technologies et prévoient notamment :

- L'interdiction générale de tels traitements et l'exception faite pour ceux mis en œuvre par la Direction de la Sûreté Publique ;
- La création de plusieurs listes d'alerte des personnes recherchées ou signalées tenues par le Directeur de la Sûreté Publique ;
- La mise en œuvre des opérations de recherche et d'identification selon des limites de temps et de lieux ;
- Des limitations pour la conservation et la consultation des données ;
- L'interdiction de l'interconnexion avec d'autres données ou fichiers.

2°/ Toutefois, le Haut Commissariat estime que le caractère sensible des données biométriques et le champ très large du projet de loi devaient appeler des garanties encore plus strictes

Ces nouveaux systèmes sont, en effet, particulièrement à risque au sens de l'article 35 de la loi n° 1.565 du 3 décembre 2024 relative à la protection des données personnelles en ce qu'ils traitent des données sensibles, impliquent surveillance systématique à grande échelle pour des finalités pouvant revêtir un caractère répressif et en utilisant des technologies particulièrement intrusives et évolutives.

Ainsi, en application de la loi précitée, ils sont éligibles aux formalités préalables prévues aux articles des articles 58 et suivants de la loi précitée.

Par ailleurs, le champ du projet de loi est particulièrement étendu et plus large que celui de la seule vidéoprotection :

En effet, la vidéoprotection s'exerce sur la voie publique.

Or, les lieux où la surveillance prévue par le projet de loi peut s'exercer sont plus larges s'agissant des « lieux accessibles au public » soumis à vidéosurveillance, définis à l'article 3 de la loi n°1.430, à savoir « tous lieux dont l'accès est libre tels que plages, jardins publics, promenades publiques, ou encore les commerces, ainsi que les lieux dont l'accès est possible, même sous condition, dans la mesure où toute

personne qui le souhaite peut remplir cette condition comme c'est notamment le cas lorsque le paiement d'un droit d'entrée est requis, par exemple au cinéma ou au musée ».

L'utilisation sur la voie publique et dans les lieux accessibles au public ne permet en outre pas aux personnes de s'opposer à leur utilisation ou de leur préférer une voie alternative car les données biométriques de chaque personne sont traitées de manière indifférenciée.

Le champ du projet de loi inclut le domaine judiciaire : il semble en effet que certaines des personnes figurant sur la liste d'alerte prévues à l'article 8-3 y figureront également à l'occasion de procédures judiciaires qui sont exclues du champ d'application de la loi n°1.430 et du chapitre VI de la loi.

Le champ du projet de loi est susceptible de viser le domaine administratif : ainsi l'article 8 -3-6°) vise les personnes faisant l'objet d'un placement : Or, tous les placements ne sont pas de nature judiciaire et toutes les personnes faisant l'objet d'un placement administratif ne représentent pas forcément un danger suffisamment imminent ou grave pour recourir à de telles mesures.

Ainsi, le Haut Commissariat estime que, dans ces cas, il devrait être précisé que l'inscription sur une liste d'alerte, hors menace grave et imminente et questions touchant à la sécurité nationale, ne peut se faire qu'en application des règles du code de procédure pénale et donc à la requête du Parquet ou d'un Juge d'instruction.

Des effets plus larges encore sur l'exercice des libertés : le rapport du Défenseur des Droits français « *Technologies biométriques : l'impératif respect des droits fondamentaux* » avait mis en évidence le risque d'effet dissuasif de la mise en œuvre de tels dispositifs qui mettent en danger, ou peuvent le laisser supposer, l'anonymat dans l'espace public (sans collecte du consentement), dans l'exercice de certains droits fondamentaux (liberté d'expression, d'aller et venir, d'assemblée, d'association).

Afin d'éviter un tel écueil, le Haut Commissariat estime que les principes devant être respectés et les garanties apportées devraient être clairement portés à la connaissance des personnes concernées afin de les rassurer pleinement quant à la préservation de leurs libertés et de ne pas les décourager de les exercer.

3°/ Or, en l'état, les dispositions du projet de loi paraissent insuffisantes pour garantir sans ambigüité aucune le respect effectif des principes identifiés en première partie

- Concernant les droits fondamentaux et les discriminations :

Droits fondamentaux :

Le projet de loi, pas plus que la loi n°1.430 ne font mention directe des risques élevés et spécifiques présentés par la mise en œuvre de systèmes de reconnaissance faciale, ni des moyens pour y remédier le cas échéant.

Ne sont pas expressément mentionnés le droit à la vie privée, à la liberté d'expression, à la liberté de réunion, le droit d'aller et venir, le droit à la liberté de pensée et d'opinion.

Le Haut Commissariat recommande donc de faire une référence directe aux textes de droit interne protégeant les droits fondamentaux et interdisant les discriminations.

Risques de discrimination :

En l'absence de loi générale en Principauté, il importe que cet aspect soit évalué pour chaque texte et particulièrement sur ce le présent projet de loi.

Or, il s'avère qu'en l'espèce, outre les questions raciale ou ethnique, il pourrait exister un risque de contrôle accru pour les personnes qui portent des lunettes, une capuche, un masque, qui pourraient se trouver assimilées à des individus voulant se soustraire à la reconnaissance faciale.

Même si elle ne figure pas explicitement dans la loi sur la protection des informations nominatives, la notion de risque de discrimination apparaît dans les articles 7 et 64 de la loi n°1.565 et une mention spécifique de la prise en compte de ce risque pourrait figurer dans le présent projet.

Enfin, l'absence de référence à des normes pour les logiciels et applications fait courir le risque que certains outils utilisés pourraient comporter des biais conduisant à discriminer certaines catégories de personnes. Même si le pourcentage d'erreur est faible (de l'ordre de 0,5% selon les sources du Défenseur des Droits français) les conséquences pour ces personnes peuvent s'avérer très lourdes.

Ainsi, le Haut Commissariat recommande de :

- **Mentionner le risque particulier de discrimination que comporte ce type de traitements et la nécessité de recourir à des garanties appropriées.**
- **Prévoir une procédure d'agrément des logiciels afin de garantir l'utilisation d'outils ne comportant pas de biais.**

➤ Concernant le principe de nécessité absolue :

Les normes européennes citées en première partie prévoient que la mise en œuvre de systèmes recourant à la reconnaissance faciale n'est possible qu'en cas de nécessité absolue pour (exemple : menaces terroristes ...). Or le projet de loi semble beaucoup moins limitatif.

La notion d'« *intérêts fondamentaux* » est trop extensive :

Certes, la loi n°1430 à laquelle il se réfère définit à son article 1^{er} la notion d'intérêts fondamentaux de la Principauté fondant l'action préventive en matière de police : « *les intérêts fondamentaux de la Principauté mentionnés à la lettre a) du précédent alinéa s'entendent, au sens de la présente loi, du maintien de son indépendance, de ses institutions, de l'intégrité de son territoire, de sa sécurité, de la sauvegarde de sa population, de l'équilibre de son milieu naturel et de son environnement, des éléments essentiels de son potentiel scientifique et économique ainsi que de son patrimoine culturel* ».

Toutefois, il semble que certains des termes de cette définition et notamment les notions d'« *équilibre de son milieu naturel et de son environnement et d'éléments essentiels de son potentiel scientifique et économique ainsi que de son patrimoine culturel* » soient trop larges ou sujets à interprétation pour être appliqués sans plus de précision dans le contexte potentiellement très attentatoire aux droits fondamentaux de la reconnaissance faciale.

La référence aux dispositions de la loi n° 1.430 ne suffit donc pas à répondre au critère de la nécessité absolue et l'absence de toute autre référence rend incertaine le respect de ce principe. Il doit plus clairement ressortir que le recours à ces systèmes doit demeurer une exception également lorsqu'ils sont utilisés par les autorités.

Les motifs d'inscription sur les listes d'alertes sont parfois trop larges :

L'article 8-3 1°) projette d'inscrire sur une liste d'alerte des personnes condamnées pour une infraction punie d'une peine supérieure ou égale à un an d'emprisonnement. Le Haut Commissariat estime ce

critère excessif compte tenu du nombre d'infractions relativement peu graves sanctionnées par ce maxima. En outre l'interpellation des auteurs de certaines de ces infractions ne présente pas toujours un caractère d'urgence au regard de la menace qu'il représente et peut parfaitement être assurée par d'autres moyens moins intrusifs. Cela pourrait aussi concerner une personne soumise à un contrôle judiciaire ou faisant l'objet d'un aménagement de peine ou d'un placement judiciaire ou administratif visé à l'article 8-3 6°).

A titre de comparaison, le Règlement européen prévoit ainsi pour sa part que « L'utilisation de ces systèmes à des fins répressives devrait être interdite, sauf dans trois situations précisément répertoriées et définies, dans lesquelles l'utilisation se limite au strict nécessaire à la réalisation d'objectifs d'intérêt général dont l'importance est considérée comme supérieure aux risques encourus. Ces situations comprennent la recherche de victimes potentielles d'actes criminels, y compris des enfants disparus, certaines menaces pour la vie ou la sécurité physique des personnes physiques, y compris les attaques terroristes, et la détection, la localisation, l'identification ou les poursuites à l'encontre des auteurs ou des suspects d'infractions pénales visées à l'annexe II du Règlement, à savoir :

- terrorisme,
- traite des êtres humains,
- exploitation sexuelle des enfants ou la pédopornographie,
- trafic de stupéfiants ou de substances psychotropes,
- trafic d'armes, de munitions ou d'explosif,
- homicide volontaire, coups et blessures graves,
- trafic d'organes et de tissus humains,
- trafic de matières nucléaires ou radioactives,
- enlèvement, la séquestration ou la prise d'otages,
- crimes relevant de la compétence de la Cour Pénale Internationale,
- détournement d'avion ou de navire,
- viol,
- criminalité environnementale,
- vol organisé ou à main armée,
- sabotage,
- participation à une organisation criminelle impliquée dans une ou plusieurs des infractions précitées.

Seules ces infractions ont été estimées suffisamment graves pour justifier l'utilisation de systèmes d'identification biométrique à distance « en temps réel » dans le Règlement européen.

S'il est compréhensible que les impératifs de sécurité spécifiques à la Principauté de Monaco justifient de ne pas reproduire à l'identique les critères retenus par l'Union européenne, il semble toutefois que le critère retenu par l'Article 8-3 1°) (infraction réprimée par plus d'un an d'emprisonnement) soit beaucoup trop large et devrait être remplacé, soit par une liste d'infractions plus précise, soit par le critère de trois ans d'emprisonnement, en prévoyant éventuellement des exceptions pour certaines infractions ou en cas de danger grave et imminent.

Le Règlement européen prévoit également que la base de données de référence des personnes devrait être appropriée pour chaque cas d'utilisation dans chacune des situations mentionnées ci-dessus.

De plus, le Haut Commissariat considère, se référant aux critères européens, que toute utilisation d'un système d'identification biométrique à distance « en temps réel » dans des espaces accessibles au public à des fins répressives devrait être subordonnée, hormis dans les cas impliquant la sécurité nationale ou une menace grave et imminente, à l'autorisation expresse et spécifique d'une autorité

judiciaire ou d'une autorité administrative indépendante. Cette autorisation devrait en principe être obtenue avant l'utilisation, sauf dans des situations d'urgence dûment justifiées, c'est-à-dire des situations où la nécessité d'utiliser les systèmes en question est de nature à rendre effectivement et objectivement impossible l'obtention d'une autorisation avant le début de l'utilisation. Dans de telles situations d'urgence, l'utilisation devrait être limitée au strict nécessaire et être assortie de garanties et de conditions appropriées et spécifiées dans le contexte de chaque cas d'utilisation urgente par les autorités répressives elles-mêmes. De plus, les autorités répressives devraient, dans de telles situations, chercher à obtenir une autorisation dans les meilleurs délais, tout en indiquant les raisons pour lesquelles elles n'ont pas pu la demander plus tôt.

Enfin, on peut considérer que, dans le contexte monégasque où il existe des moyens déjà très efficaces afin de localiser ou d'identifier les personnes, le recours à la reconnaissance faciale devrait avoir un caractère subsidiaire, réservé aux situations dans lesquelles aucune autre possibilité n'est efficace ou raisonnable, et dans tous les autres cas, des outils alternatifs moins intrusifs devraient continuer à être utilisés (cf. rapport du défenseur des Droits Français « *Technologies biométriques : l'impératif respect des droits fondamentaux* » page 17).

Le Haut Commissariat recommande à cet égard :

- **De mieux préciser les motifs pouvant donner lieu à l'utilisation de ces techniques ;**
- **De prévoir, outre la mise en place de traitements différenciés, l'utilisation de bases de données distinctes correspondant à chaque type de situations répertoriées comme nécessitant le recours à des technologies de reconnaissance faciale.**

➤ Concernant l'exigence de prévisibilité et de transparence :

En l'absence de norme interne accessible et prévisible, tout traitement d'informations nominatives ainsi mis en œuvre par l'autorité publique constitue une violation du droit au respect de la vie privée garanti par l'article 8 de la CEDH. La loi doit donc être claire quant à son champ et ses modalités d'application.

En ce qui concerne le champ de la loi, si l'exposé des motifs parle de reconnaissance faciale, le dispositif du projet de loi ne reprend pas cette expression. En effet, l'article 8-2 du projet de loi fait référence à « *un traitement automatisé de données personnelles ayant pour finalité de faciliter la détection, la recherche et l'identification des personnes recherchées ou signalées inscrites sur les listes d'alerte...* »

Par ailleurs, l'absence de description des techniques pouvant être utilisées, ou de renvoi à des textes d'application ou à des normes reconnues, peut induire en erreur sur la portée exacte de ce texte, les personnes surveillées ignorant la nature précise des technologies susceptibles de leur être appliquées et, a contrario, la nature de celles qui demeurent interdites, même pour la Direction de la Sécurité Publique. Ainsi, se pose la question de savoir si des systèmes d'évaluation (visant par exemple à déduire des intentions) ou de catégorisation (par sexe, âge, origine...) peuvent être autorisés à être mis en œuvre en vertu du présent projet de texte.

Le Haut Commissariat relève en outre que le projet de loi n'appréhende pas la question de l'usage de la reconnaissance faciale en matière de recherche des individus comme un tout, mais le scinde, dans plusieurs titres de la loi 1.430, à savoir le titre IV qui prévoit la mise à disposition des images des systèmes de vidéosurveillance et le VI bis, ce qui pose problème du point de vue de la compréhension du texte et de sa prévisibilité.

Aucune disposition n'exige par ailleurs que les personnes concernées soient informées de l'utilisation de cette technologie dans certains lieux ou à l'occasion de certains événements.

La sécurité juridique commande donc que les notions soient plus clairement explicitées dans la loi.

Enfin, le Haut Commissariat relève que, bien que son intitulé soit large, le texte ne fait aucune mention explicite de l'usage des techniques de reconnaissance faciale sur internet et les réseaux sociaux. Or, les lignes directrices sur la reconnaissance faciale du Comité de la Convention STE 108, reprises dans la jurisprudence de la CEDH (arrêt Glukhin c. Russie) mentionne expressément que « *Les législateurs et les décideurs veilleront à ce que les images disponibles en format numérique ne puissent pas être traitées pour en extraire des modèles biométriques, ou pour être intégrées dans des systèmes biométriques, afin de reconnaître la personne figurant sur les images numériques, sans base juridique spécifique pour le nouveau traitement lorsque ces images ont été capturées à d'autres fins (à partir de médias sociaux par exemple).* »

Comme l'extraction de modèles biométriques à partir d'images numériques implique le traitement de données sensibles, il convient de sécuriser la base juridique éventuelle envisagée ci-dessous qui varie selon les secteurs et les situations.

Plus précisément, utiliser des images numériques qui ont été téléchargées à partir d'internet, y compris sur les médias sociaux ou sur des sites de gestion de photos en ligne, ou qui ont été capturées via des caméras de vidéosurveillance, ne peut être considéré comme licite au seul motif que ces données personnelles ont été rendues manifestement disponibles par les personnes concernées ».

Ainsi, le Haut Commissariat recommande de prévoir l'information des usagers concernant le champ des contrôles exercés et les techniques qui seront utilisées et d'appliquer explicitement aux données recueillies sur internet et sur les réseaux sociaux les mêmes dispositions qu'aux images de vidéo-protection.

➤ Concernant l'homologation des logiciels mis en œuvre :

Le système qui doit être mis en œuvre par la Direction de la Sûreté Publique présente un double danger car il concerne à la fois des données sensibles et une utilisation à des fins répressives. Il serait donc un système à haut risque au titre de la réglementation européenne.

A ce titre, les applications qu'il utiliserait devraient être soumises à des dispositions particulières de conformité, notamment en matière de sécurité et de fiabilité, qui ne sont pas prévues par le présent projet de loi.

Le Haut Commissariat relève en outre que l'utilisation de systèmes non conformes pourrait entraîner une non adéquation avec les exigences du RGPD : en effet dans l'exposé des motifs du règlement européen est souligné l'imbrication des dispositions proposées avec celles du RGPD.

Ainsi le Défenseur des Droits français a-t-il invité les autorités françaises à s'inspirer largement de la proposition de règlement européen prévoyant que les fournisseurs de dispositifs d'identification biométrique à distance soient soumis à des obligations de respect de certaines exigences strictes en terme de transparence et d'évaluation des risques avant toute mise en service et d'une procédure d'évaluation de la conformité *ex-ante* et indépendante, ainsi qu'au long du cycle de vie (cf. rapport du Défenseur des Droits Français « *Technologies biométriques : l'impératif respect des droits fondamentaux* » page 17).

Afin de fournir les garanties appropriées concernant la mise en œuvre de ce système devraient donc être prévus :

- Un dispositif d'évaluation et de reconnaissance de conformité autonome ou lié à celui de l'UE.
- Des mesures concernant les prestataires et fournisseurs.
- Des mesures évitant les biais stigmatisant un ou plusieurs types d'individus.

Le Haut Commissariat recommande donc :

- De prévoir l'élaboration de normes et de procédures d'évaluation ou se référer à celles prévues par le droit européen afin de garantir l'usage de logiciels et d'applications sûrs.
- De mieux décrire les applications et logiciels qui seront mis en œuvre ainsi que ceux qui sont interdits, quitte à renvoyer à des textes d'application pouvant faire l'objet de mises à jour.
- De prévoir les obligations concernant les fournisseurs systèmes
- De prévoir la formation appropriée des utilisateurs du système prévu.
- De prévoir la possibilité d'imposer un moratoire ou une interdiction à l'égard de certaines applications de systèmes d'IA présentant des dangers particuliers.

➤ Recours effectif

La possibilité de recours n'est pas spécifiée dans la loi mais découle de l'application de la loi n° 1.565 du 3 décembre 2024 à laquelle renvoie l'article 6 de la loi n°1.430.

Pour que ce recours soit effectif, il faudrait toutefois que les traitements soient différenciés et qu'une information claire soit fournie aux personnes concernées.

Le Haut Commissariat recommande donc de prévoir des phases de tests préalables à toute mise en œuvre correspondant à des situations et des outils précisément définis.

CONCLUSIONS

Au plan général, le Haut Commissariat considère que l'équilibre entre sécurité d'une part et, d'autre part, la préservation de la vie privée et des droits fondamentaux est au cœur du respect des valeurs qui fondent les Institutions de la Principauté de Monaco mais aussi du maintien de son attractivité en garantissant à tous ceux qu'elle accueille la protection de leurs droits les plus essentiels.

A ce titre, le Haut Commissariat insiste plus particulièrement sur la nécessité de veiller à ce que la loi garantisse expressément que la mise en œuvre de systèmes d'identification biométrique à distance en temps réel de personnes physiques dans les espaces accessibles au public à des fins répressives soit limitée au strict nécessaire pour la réalisation d'objectifs d'intérêt général dont l'importance est considérée comme supérieure aux risques encourus en matière d'atteintes aux droits et libertés.

Le Haut Commissariat estime en outre que l'équilibre recherché devrait être évalué en tenant compte du contexte monégasque, qui garantit déjà un très haut niveau de sécurité, comme en atteste les excellents résultats présentés chaque année par la Direction de la Sûreté Publique, et en évaluant plus finement les domaines où le recours aux techniques de reconnaissance faciale permettrait de pallier les difficultés précisément identifiées et présenterait une réelle valeur ajoutée.

En effet, le Haut Commissariat souligne que la forte densité des réseaux de vidéoprotection et de télésurveillance sur l'ensemble du territoire de la Principauté pourrait, en l'absence de limitations strictes, s'assimiler à un dispositif de surveillance généralisée de la population.

Le Haut Commissariat invite par ailleurs le Conseil National à rechercher une articulation plus claire du présent projet de loi avec les textes en vigueur. Cette articulation pouvant éventuellement être trouvée en prévoyant un texte plus large traitant de la mise en œuvre des applications faisant appel à l'intelligence artificielle.

Le Haut Commissariat invite également le Conseil National à tenir d'ores et déjà compte des dispositions figurant dans les textes européens récemment entrés en vigueur en matière de régulation de l'intelligence artificielle afin d'éviter que la législation monégasque ne soit à court terme déjà plus en phase avec les standards européens.