2023-11
17 novembre 2023

PROJET DE LOI RELATIVE A L'UTILISATION DE LA VIDEOPROTECTION ET DE LA VIDEOSURVEILLANCE DES LIEUX ACCESSIBLES AU PUBLIC POUR LA DETECTION, LA RECHERCHE ET L'IDENTIFICATION DES PERSONNES RECHERCHEES OU SIGNALEES AU MOYEN DE SYSTEME D'IDENTIFICATION BIOMETRIQUE A DISTANCE.

EXPOSÉ DES MOTIFS

La préservation de la sécurité publique au bénéfice des personnes et des biens constitue, depuis longtemps déjà, l'un des piliers de la politique mise en œuvre par le Gouvernement Princier, sous la haute autorité du Prince Souverain.

Depuis 2016, cette mission régalienne fondamentale de l'État, au service de ce qui apparaît comme l'une des singularités de la Principauté et un vecteur essentiel de son attractivité, est exercée dans le cadre juridique strict institué par la loi n° 1.430 du 13 juillet 2016 portant diverses mesures relatives à la préservation de la sécurité nationale.

Succédant à l'Ordonnance du 6 juin 1867 sur la police générale, modifiée, dans le but de répondre aux exigences contemporaines que posaient tant la protection des intérêts fondamentaux de la Principauté que la lutte contre la délinquance, la loi n° 1.430 a modernisé l'arsenal juridique de l'État indispensable pour assurer cette protection, tout en préservant les droits et libertés fondamentaux des personnes tels que garantis par la Constitution.

Face à l'accroissement et à la diversification des menaces auxquels sont confrontés les services de police en charge de la protection des personnes et des biens, l'amélioration de l'efficacité des outils et techniques dont ils disposent constitue, aujourd'hui plus que jamais, un enjeu primordial pour garantir la pérennité de cette sécurité publique.

Pour y parvenir, l'automatisation de certaines tâches purement techniques en vue d'accroître l'efficacité de l'exécution de certaines missions de police se révèle indispensable, compte tenu des avantages que procurent désormais les technologies de traitement d'images. C'est particulièrement le cas de celles donnant lieu à la détection, l'identification ou encore l'authentification des personnes recherchées pour les besoins de la justice ou de la police.

Ces processus d'automatisation du traitement des images font appel aux technologies dites d'« *intelligence artificielle* », dont le vocable quelque peu sibyllin renvoie, au plan pratique, par exemple pour la norme ISO 2382-2015, aux systèmes ou programmes informatiques capables d'« *exécuter des fonctions généralement associées à l'intelligence humaine, telles que le raisonnement et l'apprentissage* ». Au plan strictement juridique, la Commission européenne a retenu, dans sa proposition de règlement établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union, du 21 avril 2021, que l'on devait considérer comme relevant des technologies d'intelligence tout logiciel pouvant « *pour un ensemble donné d'objectifs définis par l'homme, générer des résultats tels que des contenus, des prédictions, des recommandations ou des décisions influençant les environnements avec lesquels il interagit* ».

D'un point de vue plus général, nul n'ignore que ces technologies d'intelligence artificielle sont, pour des usages de notre quotidien, très utilisées par les grands acteurs de l'économie numérique, tels que Facebook, Amazon, Apple ou Google. Elles sont également de plus en plus présentes dans les lieux accessibles au public et sensibles comme les aéroports ou les gares ferroviaires et maritimes.

Réalisés grâce notamment au couplage de l'intelligence artificielle avec de nombreux capteurs tels que des caméras, des détecteurs de présence, ou des détecteurs infrarouges, ces systèmes « *intelligents* » d'automatisation des tâches sont en mesure de procéder, au moyen d'algorithmes, à une analyse d'image permettant de détecter automatiquement les mouvements de foule, un objet abandonné, ou une personne au sein d'une foule par exemple à partir d'un accessoire que celle-ci porterait comme une casquette ou des lunettes.

De nombreux pays européens ont d'ores et déjà déployé sur les zones sensibles de leur territoire des systèmes de vidéoprotection « *intelligents* », afin de renforcer la sécurisation des lieux publics, particulièrement à l'occasion d'événements générateurs de mouvements de foule importante.

En automatisant la détection de mouvements, de personnes ou d'objets suspects, ces systèmes facilitent les prises de décisions par la personne en charge de l'exploitation du système de vidéoprotection. Ils ne sont d'ailleurs conçus, dans le cadre de ces missions de protection de la sécurité publique, que comme des outils d'aide à la décision ; en cela, ils sont dépourvus de programmation susceptible de leur permettre de se substituer à l'intervention humaine lorsque celle-ci est requise.

Aujourd'hui, à la faveur des récents progrès technologiques, la vidéoprotection intelligente permet d'aller encore plus loin dans le traitement automatique des images pour parvenir à identifier ou authentifier une personne en particulier au sein d'une foule à partir des données biométriques du visage de celle-ci.

En effet, comme tout procédé biométrique, la reconnaissance faciale peut remplir ces deux fonctions distinctes, à savoir :

- l'authentification d'une personne, qui vise à vérifier que celle-ci est bien la personne qu'elle prétend être.

- l'identification d'une personne, qui vise à retrouver une personne au sein d'un groupe d'individus, dans un lieu, une image ou une base de données.

Dans les deux cas, les techniques de reconnaissance faciale reposent sur une estimation de correspondance entre des gabarits : celui qui est comparé et celui ou ceux servant d'étalon. Le processus de comparaison calcule une probabilité, plus ou moins forte, que la personne soit bien celle que l'on cherche à authentifier ou identifier ; si cette probabilité dépasse un seuil déterminé dans le système, celui-ci va considérer qu'il y a correspondance.

Le présent projet de loi s'inscrit dans le cadre de ces nouveaux usages qui aident à la détection et l'identification à distance des personnes recherchées à partir des images des systèmes de vidéoprotection déployés sur le territoire de la Principauté, et lorsque cela sera nécessaire, également par les images captées par les systèmes de vidéosurveillance des lieux accessibles au public. L'objectif étant de pouvoir automatiser certaines tâches qui sont aujourd'hui effectuées, à l'œil nu, par les opérateurs de la Direction de la Sûreté Publique chargés de l'exploitation du réseau de vidéoprotection.

En effet, l'amélioration des conditions d'exploitation des réseaux de vidéoprotection ne saurait se passer de l'assistance technologique apportée aux opérateurs en charge de ces systèmes, laquelle leur permettra de traiter plus rapidement et plus efficacement l'examen de certaines images vidéo au moyen de programmes informatiques efficients.

Pour mieux appréhender l'intérêt de cette assistance, il convient de relever que le réseau de vidéoprotection administré par la Direction de la Sûreté Publique comporte près de 1 000 caméras qui sont exploitées toute l'année par des fonctionnaires de police, 24 heures sur 24. Or, ces fonctionnaires doivent aussi assurer simultanément plusieurs autres tâches, à la fois complexes et tout aussi essentielles que l'identification des personnes recherchées, telles que la coordination des interventions de police ou la gestion des appels d'urgence dits « *police-secours* ». La nature de leurs fonctions de police ne permet donc pas de dédier ces agents, de manière exclusive, à l'exploitation des images du réseau de vidéoprotection.

Aussi est-il nécessaire de pouvoir avoir recours aux outils modernes d'aide à l'identification des personnes recherchées par la police ou la justice, laquelle peut de nos jours être réalisée tant sur des images captées en temps réel, c'est-à-dire sur les images des caméras de vidéoprotection diffusées en direct, comme en temps différé, c'est-à-dire sur celles enregistrées au préalable par le système.

Cependant, compte tenu des enjeux tenant à la préservation des libertés publiques, il a paru opportun au Gouvernement Princier de privilégier le recours à la loi, pour déterminer le cadre juridique le plus pertinent pour une mise en œuvre efficace, proportionnée et transparente du traitement de données dans lequel a vocation à s'inscrire la technologie d'identification biométrique à distance projetée par le présent texte et appelée à être mise en œuvre par la Direction de la Sûreté Publique pour l'automatisation de certaines tâches, permettant de retrouver les personnes recherchées qui seront inscrites sur une liste d'alerte dédiée à cet effet.

La législation monégasque projetée se veut pionnière dans ce domaine, car pour l'heure, les projets législatifs à l'étude dans les pays européens et au niveau de l'Union européenne n'ont pas encore abouti à des règles harmonisées propres aux traitements de données relatifs à l'identification biométrique à distance des personnes recherchées dans les lieux accessibles au public.

Pour les pays membres de l'Union européenne, le cadre juridique applicable à cette situation est, pour l'essentiel, celui du droit commun de la protection des données personnelles, lequel englobe les dispositions du Règlement (UE) 2016/679 du 27 avril 2016, dit Règlement général sur la protection des données ou R.G.P.D. et celles de la Directive (UE) 2016/680 du 27 avril 2016, dite Directive « *Police-Justice* », dont les dispositions s'appliquent en particulier aux traitements de données mis en œuvre par les services de police et les services judiciaires.

Les données biométriques constituant des données sensibles, leur traitement n'est donc autorisé par le droit de l'Union européenne qu'en cas de nécessité « *absolue* ». Si ce cadre juridique se veut particulièrement restrictif, on observera que le droit de l'Union est assez peu explicite sur les exigences tenant à ce caractère « *absolu* » à même de justifier de l'opportunité de la mise en œuvre de traitements de données relatifs à l'identification biométrique à distance des personnes recherchées dans les lieux accessibles au public pour des impératifs de sécurité publique.

Aussi plusieurs États membres ont-ils engagé des réflexions visant à préciser dans leurs législations internes les conditions et modalités qui permettront de recourir aux technologies de reconnaissance faciale notamment dans l'espace public par les services de police. C'est par exemple le cas en France, où plusieurs propositions de loi sur ce sujet ont été déposées, mais sans pour autant que celles-ci n'aient à ce jour donné lieu à l'institution d'un cadre législatif propre à cette problématique.

En parallèle des réflexions conduites au sein des États membres, la Commission européenne s'est elle aussi saisie de ces questions en vue d'instituer un cadre juridique uniforme au niveau de l'Union européenne. Le cadre envisagé vise en revanche, de manière plus large, l'ensemble de la chaîne industrielle, depuis la création jusqu'à l'utilisation des systèmes d'intelligence artificielle.

Les travaux de la Commission ont abouti à la communication au Parlement européen et au Conseil de l'Union européenne, le 21 avril 2021, d'une proposition de règlement européen établissant des règles harmonisées concernant l'intelligence artificielle, dit « *Artificial Intelligence Act* » ». Les dispositions de cette proposition de règlement insistent sur les conditions du recours aux systèmes d'identification biométrique à distance, à l'instar de la reconnaissance faciale, dans les espaces accessibles au public. Ce texte propose de permettre l'utilisation de ces systèmes par les services de police pour la recherche de victimes de crime, les enfants disparus ou la prévention de menaces graves pour la sécurité des personnes, telles que les attaques terroristes ou encore la détection et l'identification d'auteur ou de suspect d'infractions graves.

Compte tenu de ce contexte européen où les standards juridiques sont encore en voie de consolidation, les cas d'usage de la reconnaissance faciale à distance par les services de police dans les espaces accessibles au public demeurent circonscrits à des lieux sensibles, tels que les aéroports ou certaines gares ferroviaires pour, par exemple, faciliter la réalisation des formalités requises pour le passage des frontières comme dans le cadre du dispositif français dénommé « PARAFE ».

Ce contexte a tout de même permis de mener en Europe des expérimentations à plus grande échelle qui ont confirmé l'efficacité de ces systèmes d'identification, dans l'attente de l'adoption de dispositions législatives propres à ces usages qui permettrait d'y avoir recours de manière pérenne dans le respect des droits et libertés fondamentaux des personnes concernées.

Parmi les expérimentations notables, on notera que les technologies d'identification biométrique à distance ont été mises en œuvre en Allemagne lors du G20 de 2017 à Hambourg, ainsi qu'en France à l'occasion du Carnaval de Nice en 2019. La reconnaissance faciale à distance a aussi été déployée par les services de police jusqu'en 2021 en Suède et au Royaume-Uni. Ces dernières expérimentations ont toutefois dû être interrompues à la suite des décisions de l'autorité de protection des données suédoise et des tribunaux anglais en raison notamment des conditions de mise en œuvre de ces traitements de données sensibles insuffisamment protectrices des droits et libertés fondamentaux des personnes concernées.

Ainsi observe-t-on que l'absence de base légale claire, précise et propre aux conditions d'usage des technologies d'identification à distance dans les lieux accessibles au public pour des finalités tenant à la préservation de la sécurité publique fait obstacle à leur utilisation pérenne, ce alors même que l'aide que ces technologies est susceptible d'apporter aux services de police pour maintenir un haut niveau d'efficacité dans la réalisation de leurs missions est désormais avérée.

C'est pour ces raisons, et en parallèle du projet de loi n° 1.054 relative à la protection des données personnelles qui a vocation à succéder à la loi n° 1.165 du 23 décembre 1993 relative à la protection des informations nominatives, modifiée, que l'élaboration du présent projet de loi a été souhaitée.

Compte tenu de son objet spécifique, le dispositif juridique projeté viendra compléter les dispositions d'origine de la loi n° 1.430 du 13 juillet 2016, précitée, et limitera de fait les cas de recours aux technologies d'identification biométriques à distance dans les espaces accessibles au public aux seules finalités impérieuses de préservation de la sécurité nationale prévue par ladite loi. L'objectif est celui de fixer un cadre juridique aussi protecteur des droits et libertés fondamentaux des personnes concernées, qu'efficace pour leur mise en œuvre par les agents habilités de la Direction de la Sûreté Publique affectés à l'exploitation des images des systèmes de vidéoprotection.

Pour répondre au mieux à ces enjeux, il est prévu qu'outre les garanties spécifiques prévues par le présent projet de loi pour la protection des droits fondamentaux des personnes concernées, les garanties prévues par le droit commun de la protection des données personnelles – à savoir, pour l'heure, celles de la loi n° 1.165 du 23 décembre 1993, modifiée, précitée – seront également applicables au traitement de données relatif aux images des systèmes de vidéoprotection et de vidéosurveillance des espaces accessibles au public. Il convient à cet égard de relever que ces garanties sont, en outre, accompagnées de dispositions spécifiques, relatives aux traitements de données personnelles portant sur des soupçons d'activités illicites, des infractions ou des mesures de sûreté, comportant des données biométriques nécessaires au contrôle de l'identité des personnes ou mis en œuvre à des fins de surveillance.

Sous l'empire de la loi n° 1.165, on rappellera qu'un traitement de données biométriques concernant la sécurité publique ne peut, en principe, être mis en œuvre par la Direction de la Sûreté Publique ou la Direction des Services Judiciaires sans qu'ait été recueilli au préalable l'avis de la Commission de Contrôle des Informations Nominatives (C.C.I.N.) sur le caractère adéquat des garanties apportées à la protection des droits et libertés fondamentaux des personnes concernées par le traitement en question.

A cet égard, les autorités administratives et judiciaires sont particulièrement attentives aux avis et recommandations de la C.C.I.N., témoignant d'un attachement commun des acteurs concernés quant à la préservation des droits et libertés fondamentaux dans le domaine des nouvelles technologies de la communication et de l'information, attachement sur lequel reposent la coopération et le dialogue entre l'autorité de protection des données et les services administratifs et judiciaires.

C'est la raison pour laquelle, le Gouvernement Princier a souhaité, pour l'avenir, maintenir le mécanisme de la demande d'avis de l'autorité de protection des données préalable à la mise en œuvre de tout traitement relatif à la prévention, la détection, les enquêtes et poursuites en matière d'infractions pénales. Il en sera d'ailleurs de même pour tout traitement des données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes mis en œuvre par les autorités administratives.

C'est toujours dans un esprit de coopération que la construction du dispositif du présent projet de loi s'est faite, à la faveur des différents échanges intervenus avec la C.C.I.N. laquelle avait très tôt appelé l'attention du Gouvernement Princier sur la nécessité d'engager un débat public quant à l'opportunité et au périmètre de la mise en œuvre de technologie de reconnaissance faciale dans l'espace public pour les finalités de sécurité publique.

Aussi, sur la base de l'ensemble de ces considérations, le dispositif du présent projet de loi s'est concentré sur les éléments de nature à garantir un équilibre entre les impératifs de préservation de la sécurité publique et des libertés publiques, lesquels s'articulent sur les points suivants :

- seul le traitement de données prévu par la loi permettra d'utiliser les technologies d'identification biométrique à distance dans les lieux accessibles au publics ;

- le droit commun de la protection des données, et donc les garanties fortes qu'il prévoit, viendra régir ce traitement de données relatif à l'identification biométrique à distance ;

- seules les finalités de sécurité publique impérieuses, visant à faciliter l'identification des personnes recherchées pour des motifs présentant une gravité certaine, permettront aux services de police d'avoir recours à l'identification biométrique à distance ;

- la durée de conservation limitée des données biométriques sera déterminée par la loi ;

- nul ne sera autorisé à consulter les données n'ayant pas établi de correspondance avec l'identification des personnes recherchées, sauf pour les cas et dans les conditions prévues par la loi ;

- l'absence d'interconnexion de ce traitement de données avec tout autre traitement de données personnelles mis en œuvre par la Direction de la Sûreté Publique sera assurée.

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, sans que soit obérée la possibilité pour les services compétents de mettre en œuvre ces technologies nouvelles pour les assister, dans l'exercice de leurs missions régaliennes de préservation de la sécurité publique.

Sous le bénéfice de ces observations d'ordre général, le présent projet de loi appelle les commentaires particuliers ci-après.

***

Du point de vue formel, le projet de loi est composé de 4 articles, dont les deux derniers introduisent deux nouveaux titres au sein de la loi n° 1.430 du 13 juillet 2016, à savoir un « *Titre IV bis* » prévu par l'article 3 du projet de loi, et un « *Titre VI bis* » introduit par l'article 4 du projet de loi et composé de 8 articles numérotés 8-1 à 8-8.

L'article premier du projet de loi complète les finalités pour lesquelles la vidéoprotection peut être mise en œuvre. Il prévoit l'ajout d'un chiffre 10°) au premier alinéa de l'article 5 de la loi n° 1.430 du 13 juillet 2016, visant à permettre d'utiliser la vidéoprotection pour la détection, la recherche et l'identification des personnes recherchées ou signalées inscrites sur une liste d'alerte spécifique, au moyen de technologies d'identification biométrique à distance.

Il s'agit d'autoriser le recours à ces technologies pour détecter, rechercher et identifier des personnes recherchées ou signalées pour des motifs tenants à la protection de la sécurité publique, de la sécurité nationale, de la préservation de l'ordre public ou la prévention et la détection des infractions pénales, conformément aux dispositions du nouveau Titre VI bis qui sera introduit au sein de la loi n° 1.430.

Ce cas de recours à la vidéoprotection n'est pas nouveau par sa nature mais par la méthode de sa mise en œuvre, puisque la vidéoprotection est bien entendu déjà utilisée pour détecter, rechercher ou d'identifier des personnes recherchées ou signalées pour des motifs tenant notamment à la protection de la sécurité publique ou la sécurité nationale. Seulement, ces missions sont aujourd'hui effectuées au moyen de la seule méthode du visionnage attentif de chaque seconde d'images captées par les caméras installées sur le territoire de la Principauté.

Ce travail d'identification procède de deux manières : soit il est réalisé en temps réel, c'est-à-dire en visionnant les enregistrements des images des caméras de vidéoprotection en direct ; soit il est réalisé en temps différé, c'est-à-dire en visionnant les enregistrements des images provenant de ces caméras. Tel est notamment le cas lorsque la démarche d'identification s'inscrit dans le contexte de la recherche de l'auteur d'une infraction. Ces tâches sont aujourd'hui réalisées de manière manuelle, au travers de l'œil des opérateurs. Il s'agit du reste d'un travail extrêmement fastidieux et naturellement imparfait compte tenu du nombre de personnes à rechercher et du nombre de caméras susceptibles d'être exploitées dans le cadre de cette identification.

A titre d'exemple, si les opérateurs recherchent le visage d'un malfaiteur sur 10 caméras pendant un créneau de temps de 10 heures pour déceler son éventuelle présence à l'occasion de repérages, cela nécessite 100 heures de visionnage d'enregistrements vidéo. À la différence, les outils technologiques de reconnaissance biométrique à distance permettent de réduire ce délai à quelques secondes, lorsque les conditions techniques sont réunies.

C'est ainsi à la lumière des capacités techniques qu'offrent ces technologies qu'apparaissent les limites de l'efficacité des tâches réalisées exclusivement par des opérateurs. Ces dernières peuvent du reste toujours exposer à une marge d'erreur non négligeable, compte tenu de la dimension éminemment subjective des opérations de comparaison entre les caractéristiques du visage de la personne recherchée et celles de la personne identifiée.

À la différence, les outils d'analyse biométrique des images permettent non seulement d'accroître le nombre des identifications, mais également d'avoir un meilleur taux d'identification des personnes, étant précisé que chaque identification fait nécessairement l'objet d'une validation *in fine* par un opérateur. En définitive, ces outils permettent d'atteindre bien mieux l'objectif d'exactitude de l'identification que ce que permet l'œil humain.

C'est pourquoi il est projeté d'insérer un chiffre 10°) nouveau à l'article 5 de la loi n° 1.430 du 13 juillet 2016, précitée, en vue d'autoriser la mise en œuvre des technologies d'identification biométrique sur les images des systèmes de vidéoprotection afin d'automatiser, en partie, le processus d'identification des personnes recherchées, et ainsi améliorer l'efficacité des opérations de recherche.

Dans le cadre de ces opérations de recherche toutefois, et comme le prévoit déjà le droit actuellement en vigueur, les technologies de reconnaissance biométriques ne pourront être utilisées sur les lieux privatifs, lesquels demeureront hors du spectre de la vidéoprotection.

L'article 2 du projet de loi prévoit d'insérer un cinquième et avant-dernier alinéa à l'article 5 de la loi n° 1.430 du 13 juillet 2016, précitée, pour tenir compte de la répartition des systèmes de vidéoprotection déployés sur le territoire de la Principauté entre plusieurs autorités administratives compétentes.

Pour les besoins des opérations d'enquête visant à la détection et l'identification des personnes recherchées, les images des systèmes de vidéoprotection de ces autorités administratives compétentes – qui ne sont pas exploités par la Direction de la Sûreté Publique – lui seront transmises afin qu'elle puisse, lorsque cela est nécessaire, y appliquer les technologies d'identification biométrique. Car à la différence de ce que prévoit l'article 5 de la loi n° 1.430 pour le déploiement des caméras de vidéoprotection, lequel peut être fait par toute autorité administrative compétente autorisée par le Ministre d'État, la mise en œuvre d'une technologie de reconnaissance biométrique à distance ne pourra être réalisée que par les fonctionnaires de la Direction de la Sûreté Publique spécialement habilités à cet effet, et pour les seuls motifs prévus par la loi.

L'article 3 du projet de loi a pour objet d'introduire un nouveau Titre *IV bis* au sein de la loi n° 1.430, composé d'un article unique « *5 bis* » relatif à la vidéosurveillance des lieux accessibles au public. Dans le sillage des différents échanges intervenus avec la C.C.I.N., cette disposition prévoit que la mise en œuvre de tout système de vidéosurveillance – à savoir les caméras déployées par des personnes physiques ou morales de droit privé, captant des images d'espaces publics – doit être préalablement autorisé par le Ministre d'État.

Sont ainsi désignés « *lieux accessibles au public* », tous lieux dont l'accès est libre tels que les 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.

En revanche, seules les images de vidéosurveillance des lieux accessibles au public pourront être transmises à la Direction de la Sûreté Publique. Ne pourront donc faire l'objet de cette transmission, les images des espaces réservés à l'usage privatif des occupants de l'immeuble concerné, tels que par exemple, les espaces réservés à la restauration ou au temps de pause des salariés pour les lieux de travail comme les centres commerciaux, cinémas ou casinos.

Eu égard notamment à l'évolution des techniques en la matière et à la spécificité des systèmes de vidéosurveillance qui seront concernés, les conditions de la transmission à la Direction de la Sûreté Publique des images des espaces publics filmés par ces systèmes seront précisées par arrêté ministériel.

Par cette transmission, outre l'objectif de permettre aux fonctionnaires de police d'assurer les missions régaliennes de préservation la sécurité publique dont ils assument la charge, la Direction de la Sûreté Publique pourra appliquer à ces images, lorsque les opérations d'enquête l'exigeront, les technologies de reconnaissance biométrique à distance visant à la détection et l'identification des personnes recherchées ou signalées.

L'article 4 du projet de loi vise également l'insertion d'un nouveau Titre « *VI bis* » au sein de la loi n° 1.430, précitée, composé de 8 articles, numérotés 8-1 à 8-8, qui créeront un cadre spécifique 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 de vidéosurveillance.

À cet égard, l'article 8-1 qui sera inséré dans le corpus juridique général de la loi n° 1.430 consacre le principe de l'interdiction du recours à toute technologie de reconnaissance biométrique à distance sur les images captées par les systèmes de vidéoprotection et de vidéosurveillance filmant les lieux accessibles au public.

Il s'agit d'interdire la possibilité pour toute autorité administrative, autre que la Direction de la Sûreté Publique, ainsi qu'à toute personne physique ou morale régulièrement autorisée à filmer les lieux accessibles à public, d'appliquer aux images qu'elles collectent un traitement de données biométriques permettant d'identifier les personnes physiques qui se situeraient dans ces lieux.

L'usage de ce type de technologie ne saurait en effet être banalisé dans l'espace public pour des motifs qui ne seraient pas impérieux pour la préservation de la paix et de l'ordre public. Pour ces raisons, ce principe d'interdiction tend à créer un régime spécifique qui ne saurait être ni contourné, ni minimisé par le droit commun de la protection des données personnelles.

Dès lors qu'un traitement de données biométriques aura pour objet ou pour effet d'identifier, au moyen de la vidéoprotection ou de la vidéosurveillance, des personnes se trouvant dans des lieux publics, celui-ci tombera sous le coup du principe d'interdiction prévu par cet article 8-1 de la loi n° 1.430, sans que les dispositions de la loi n° 1.165 du 23 décembre 1993, modifiée, précitée, ne puissent y faire échec.

Il importe ici de revenir sur les raisons ayant conduit le Gouvernement Princier à ne pas avoir inséré une telle interdiction au sein du projet de loi n° 1.054 relative à la protection des données personnelles déposé sur le bureau du Conseil National le 20 décembre 2021. Sans doute pourra-t-on observer que, du point de vue calendaire, une première justification s'évince de ce que, l'étude du présent projet de loi n'étant pas finalisée au moment du dépôt du projet de loi n° 1.054, un tel ajout eu probablement été à l'époque prématuré. Mais la raison principale tient surtout au fait que le Gouvernement Princier a estimé plus cohérent d'introduire cette interdiction dans un projet de loi qui fut, d'une part, spécifiquement dédié à la problématique de l'usage des technologies d'identification biométrique à distance dans l'espace public et, d'autre part, spécialement fondé sur une modification de la loi n° 1.430 du 13 juillet 2016, précitée, dès lors que seules les finalités prévues par cette législation paraissent légitimement à même de faire exception à l'interdiction d'utiliser les systèmes de vidéoprotection ou de vidéosurveillance pour y mettre en œuvre des technologies permettant l'identification biométrique à distance des personnes filmées dans les lieux accessibles au public. En toute occurrence, il convient dès lors de veiller à maintenir la cohérence entre ces deux cadres législatifs distincts mais néanmoins complémentaires.

La complémentarité ainsi voulue entre le droit commun de la protection des données et le droit spécial en matière d'identification biométrique à distance des personnes recherchées pour les finalités de sécurité publique ou nationale devrait trouver son point d'orgue à l'occasion du contrôle de la mise en œuvre du traitement de données objet du présent projet de loi. Dans ce cas en effet, nonobstant l'application des dispositions nouvelles de la loi n° 1.430 à ce traitement, le contrôle de sa mise en œuvre demeurera de la compétence de l'autorité de protection instituée par la législation de droit commun relative à la protection des données personnelles.

En effet, le présent projet de loi ne prévoit pas, pour le contrôle du traitement qui sera mis en œuvre par la Direction de la Sûreté Publique, l'exclusion de la compétence de la C.C.I.N. ou de l'autorité qui lui succédera. Il appartiendra donc à celle-ci, si elle devait constater un manquement à l'interdiction prévue par l'article 8-1 – ou à n'importe quelle autre disposition du Titre VI bis – à l'occasion du contrôle de la mise en œuvre du traitement par cette Direction, de prononcer les sanctions prévues par le droit commun, comme elle le fait pour les personnes physique ou morale de droit privé ou de droit public.

En outre, et aux fins de garantir l'effectivité de l'interdiction instituée par l'article 8-1, une infraction spécifique est prévue à l'article 8-8 qui a pour objet de sanctionner toute personne, autre que le personnel habilité de la Direction de la Sûreté Publique, qui, en méconnaissance des dispositions du titre VI bis, mettrait en œuvre un traitement de données personnelles utilisant les images prises par les systèmes de vidéoprotection ou de vidéosurveillance visant à identifier à distance au moyen de leurs données biométriques les personnes filmées dans des lieux accessibles au public. Une telle sanction vise principalement les personnes, physique ou morale, autorisées à installer un système de vidéosurveillance filmant les lieux accessibles au public, et qui mettrait en œuvre un traitement de données sur les images des personnes filmées sur ces lieux accessibles au public en vue de les identifier en méconnaissance de l'exception prévue au seul bénéfice de la Direction de la Sûreté Publique pour lui permettre de remplir ses missions régaliennes impérieuses.

L'article 8-2 précise la nature de l'exception à l'interdiction de mettre en œuvre un traitement automatisé des images issues des systèmes de vidéoprotection et des systèmes de vidéosurveillance des lieux accessibles aux fins d'identifier, par tout système d'identification biométrique à distance, les personnes qui se trouveraient dans ces lieux publics.

Cette exception est exclusivement prévue pour le Directeur de la Sûreté Publique, en qualité de responsable du traitement, pour la bonne exécution de ses missions de police administrative ou de police judiciaire, lesquelles sont limitativement précisées par ce projet de loi pour les motifs tenant à la protection de la sécurité publique, la sécurité nationale, la protection des personnes vulnérables et la coopération internationale et l'entraide judiciaire.

Les traitements automatisés de données qui seront ainsi mis en œuvre auront une finalité précise et délimitée par la loi en vue d'apporter l'aide technologique nécessaire aux services de police pour l'exécution de leurs missions de recherche et d'identification de personnes déterminées. Cette aide sera fournie par un logiciel d'analyse d'images permettant d'automatiser certaines tâches d'identification des personnes recherchées qui seront inscrites sur une liste spécifique, dite liste d'alerte. Ainsi, ces traitements ne concerneront nullement les personnes qui ne figureront pas sur ces listes d'alerte et qui ne font l'objet d'aucune recherche.

D'un point de vue technique, l'objectif est de procéder à une identification par comparaison des gabarits du visage des personnes recherchées dont disposera la Direction de la Sûreté Publique avec les gabarits des images capturées par les réseaux de caméras de vidéoprotection, ou, dans une moindre mesure, des caméras de vidéosurveillance filmant les espaces publics. Cette comparaison pourra être effectuée sur des images diffusées en direct comme sur celles enregistrées par le système pour les zones pré-délimitées du territoire où la recherche présente un intérêt.

Ce traitement automatisé sera mis en œuvre dans le respect des prescriptions du droit commun de la protection des données personnelles, à savoir, pour l'heure, la loi n° 1.165 du 23 décembre 1993, modifiée, précitée, puis de celles de la législation qui lui succédera, ce en vue de garantir un niveau élevé de protection des droits et libertés fondamentaux pour les personnes qui seront concernées par ce traitement de données.

S'agissant de l'article 8-3, on observera que le premier alinéa vient préciser de manière limitative les listes d'alerte qui devront être établies par le Directeur de la Sûreté Publique et, partant, les motifs pour lesquels les personnes recherchées ou signalées seront amenées à faire l'objet d'une inscription sur l'une ou plusieurs de ces listes.

Aussi, un arrêté ministériel déterminera les éléments d'identification de ces personnes et, pour chacune de ces listes, la durée de leur inscription sur celles-ci, étant précisé que cette durée devra être fixée en considération du motif pour lequel la liste dont s'agit est établie.

Plus précisément, les points 1 à 4 du premier alinéa viennent lister les motifs d'inscription qui résulteront des activités judiciaires de la Direction de la Sûreté Publique. Ces inscriptions seront réalisées dans le cadre d'enquêtes judiciaires, qui, selon les dispositions du Code de procédure pénale, sont conduites sous le contrôle de l'autorité judiciaire, afin d'identifier ou d'interpeller les auteurs d'infractions.

Il a paru expédient de fixer dans la loi le seuil de gravité de ces infractions pour des considérations tenant au respect du principe de proportionnalité dont les prescriptions encadrent l'utilisation de technologies potentiellement attentatoires à la vie privée. À cet effet, cette inscription ne pourra avoir lieu que lorsque l'infraction concernée est punie d'une peine d'emprisonnement supérieure ou égale à un an.

Il parait en outre souhaitable que puissent être inscrits sur une liste d'alerte établie à cet effet, pendant le temps strictement nécessaire à leur recherche, les mineurs en fugue ou qui ont échappé à la vigilance de leurs parents, ou encore les personnes dont la disparition inquiétante a été signalée aux services de police. L'utilisation de cette technologie permettra de retrouver plus facilement ces personnes potentiellement en danger ou en difficulté pour les remettre à leur famille.

À titre subsidiaire, pourront également y être inscrites les personnes dont la recherche ou le suivi répondent aux objectifs de sauvegarde des intérêts fondamentaux de la Principauté tels que définis au deuxième alinéa de l'article 9 de la loi n° 1.430, à savoir notamment : *« la prévention du terrorisme, de la criminalité et de la délinquance organisées ainsi que de la prolifération des armes de destruction massive* […] *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* […] *le maintien de son indépendance et de ses institutions, l'intégrité de son territoire* ».

On rappellera à cet égard que la Principauté est complètement enclavée dans le département français des Alpes-Maritimes qui a été durement frappé au cours de ces dernières années par les évènements terroristes. Sans que l'utilisation de cette nouvelle technologie permette de supprimer tout risque, il s'agit incontestablement d'un outil qui permettra d'enrichir la palette des moyens susceptibles de contribuer à la prévention et au suivi de ces phénomènes.

De la même manière, la situation géographique et politique de la Principauté, son cosmopolitisme et son attractivité économique, peuvent l'exposer à des risques résultant des tensions internationales. À cet égard, la Direction de la Sûreté Publique devrait pouvoir être en mesure de disposer d'outils de nature à prévenir au mieux toute forme d'ingérence étrangère.

Le point 5 du premier alinéa de l'article 8-3 tend à permettre l'inscription, sur une liste d'alerte établie à cet effet, de personnes qui sont l'objet d'une mesure de police administrative du Ministre d'État prise au titre de la préservation de la sécurité des biens et des personnes ou de la sécurité des grands évènements nationaux, sportifs ou culturels notamment. Cette inscription serait effectuée pour des durées variables, même parfois très brèves, selon la nature du motif justifiant cette inscription.

Par ailleurs, le Directeur de la Sûreté Publique pourra également procéder à l'inscription, sur ces listes, des personnes signalées ou recherchées à l'étranger pour l'un 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.

Enfin, conformément au point 6 du même alinéa, une liste d'alerte devra être établie à l'effet de répertorier, pour les durées les plus longues, les personnes qui sont visées par des mesures de refoulement du territoire de la Principauté, édictées en raison du risque que leur présence représente en raison de leur radicalité, de leur lien avec le crime organisé, ou en raison d'un passé judiciaire trop conséquent.

Tel pourrait par ailleurs être aussi le cas des personnes qui sont visées par une mesure d'hospitalisation d'office et qui représentent une menace grave et imminente pour les tiers.

À l'occasion de grands évènements, il pourrait enfin être envisagé l'utilisation de ces nouveaux outils technologiques afin d'améliorer la sécurité des biens et des personnes, et s'assurer de l'application des éventuelles mesures administratives ou judiciaires qui tendent à prévenir la survenance de troubles graves à l'occasion des rassemblements importants.

À titre d'exemple, les phénomènes de « *supportérisme* » violent ou les mouvements radicaux pourraient entrer dans le périmètre de cet article, sous réserve que les mesures envisagées soient proportionnées, dans le temps et dans l'espace, aux objectifs poursuivis.

Ainsi, les supporters violents d'une équipe visiteuse qui seraient visés par une mesure de police du Ministre d'État pourraient faire l'objet d'une inscription sur une liste d'alerte établie à cet effet, pendant le temps strictement nécessaire au bon déroulement de la manifestation sportive et dans l'ensemble du périmètre du stade Louis II. Il pourrait en être de même pour les personnes faisant l'objet d'une interdiction judiciaire de stade, pendant le seul temps des rencontres de football et dans le seul périmètre du stade.

De la même manière, les personnes qui ne jouissent pas de la plénitude de leurs facultés mentales et qui représentent un risque pour les personnalités de la Famille Princière pourraient faire l'objet d'une inscription pendant le temps des manifestations publiques ou privées et dans le périmètre géographique de l'évènement où la Famille Princière se rendrait.

Les personnes ainsi inscrites sur les listes d'alerte devront y être retirées par les fonctionnaires de police en charge de la mise en œuvre du traitement dès le moment, soit le motif de leur inscription n'est plus établi, soit la finalité poursuivie par leur inscription est atteinte.

En outre, il appartiendra, en tout état de cause, au Directeur de la Sûreté Publique de s'assurer, par un contrôle périodique mensuel de l'ensemble des inscriptions sur les listes d'alerte, de la validité et de la pertinence du maintien de chacune des inscriptions.

En conséquence, un enfant perdu sera ainsi radié de la liste sur laquelle il a été inscrit aussitôt qu'il aura été retrouvé par exemple. Pareillement, le supporter violent sera radié de la liste sur laquelle il a été inscrit dès que la rencontre de football aura cessé, et la personne visée par une mesure de refoulement en sera retirée dès que la mesure aura été suspendue ou abrogée, ou au plus tard à l'occasion du contrôle mensuel des inscriptions qui sera fait par le Directeur de la Sûreté Publique.

Ces règles seront déclinées dans le cadre d'un arrêté ministériel, qui viendra préciser, pour chacun des motifs d'inscription sur une liste d'alerte, la durée d'inscription sur chacune de ces listes, étant observé que, dans le sillage des dispositions prévues à l'article 8-4, celle-ci aura incidemment pour effet de limiter, dans le temps, la mise en œuvre des opérations de détection, de recherche et de détection prévues à l'article 8-2.

L'on observe ainsi que cet article portera au cœur de la loi l'exigence de proportionnalité requise lors des opérations de police visant à détecter, rechercher et identifier les personnes recherchées ou signalées sur les images de vidéoprotection et de vidéosurveillance au moyen du système d'identification biométrique à distance. Les opérations donnant lieu à l'utilisation de ce système ne pourront en effet être réalisées de manière permanente sur l'ensemble du territoire de la Principauté. Des limites de temps et de lieu en rapport avec l'objet de l'inscription sur les listes d'alerte devront être établies et appliquées pour chaque personne recherchée ou signalée inscrite sur ces listes.

L'article 8-5 détermine les conditions dans lesquelles les données qui ne correspondent pas à un rapprochement positif avec une liste d'alerte pourront être consultées. Compte tenu des atteintes que la consultation de ces données pourraient portées au droit au respect à la vie privée, il a été jugé nécessaire de limiter cette consultation aux situations les plus graves.

Ainsi, outre les infractions pénales punies d'une peine supérieure ou égale à un an d'emprisonnement et la préservation des intérêts fondamentaux de la Principauté entendus dans leur sens le plus restrictif, seuls les risques d'atteintes graves aux personnes pourront justifier une telle consultation.

L'article 8-6 vise pour sa part à encadrer les conditions de l'archivage des rapprochements positifs qui, sauf exceptions, ne devrait pas excéder trente jours. En effet, seules les enquêtes pénales pour des infractions graves, et les cas où la préservation des intérêts fondamentaux de la Principauté en regard de ses engagements internationaux le requiert, justifieront que les rapprochements positifs soient conservés au-delà de ce délai de trente jours.

Le dernier alinéa de cet article prévoit le contrôle systématique d'un agent habilité à cet effet de tout rapprochement positif par le système d'identification biométrique à distance avec les données des personnes inscrites sur une liste d'alerte. Cette disposition s'inscrit ainsi dans le sillage des obligations internationales de la Principauté, dans le cadre du Conseil de l'Europe, notamment au titre de la convention modernisée pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, du 18 mai 2018, dite « Convention 108+ ».

Dans ce cadre en effet, il est reconnu à toute personne le droit de ne pas être soumise à une décision l'affectant de manière significative, qui serait prise uniquement sur le fondement d'un traitement automatisé de données. Il s'agit d'un droit qui constitue plus largement un principe général du droit de la protection des données personnelles partagé tant par le Conseil de l'Europe que par le l'Union européenne, où des règles particulières sont en effet prévues par le R.G.P.D. et la Directive « *Police-Justice* » pour encadrer, de manière stricte, les situations donnant lieu à des décisions entièrement automatisées.

En garantissant l'intervention humaine systématique, l'article 8-6 tend à assurer un niveau de contrôle élevé des rapprochements positifs afin de garantir que les droits des personnes ne subiraient pas une atteinte injustifiée en raison de biais ou d'erreur qui seraient commises par la technologie utilisée. On relèvera toutefois que les progrès techniques accomplis au cours de ces dernières années permettent de garantir un niveau de fiabilité très élevé aux solutions logicielles mises actuellement sur le marché. Dans les conditions de fonctionnement optimales, les performances de ces solutions réduisent le risque d'erreur à un niveau bien inférieur à celui de l'œil humain.

Quoi qu'il en soit, compte tenu des enjeux liés à la protection de la vie privée et des conséquences sur les droits des personnes, le projet de loi a entendu prescrire, pour chaque rapprochement positif, une analyse et une conformation de ce rapprochement par des personnels habilités et formés à cet effet.

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 les listes 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 les listes d'alerte, laquelle fonctionnera selon des conditions d'inscription, de mise à jour et d'effacement strictement définies par la loi et les textes d'application de celle-ci.

Tel est l'objet du présent projet de loi.

***

PROJET DE LOI

Article premier

Est inséré, après le chiffre 9° du premier alinéa 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, un chiffre 10° rédigé comme suit :

« *10° - la détection, la recherche et l'identification des personnes recherchées ou signalées conformément aux dispositions du Titre VI bis.* »

Article 2

Est inséré, après le second tiret du quatrième alinéa de l'article 5 de la loi n° 1.430 du 13 juillet 2016, précitée, un cinquième alinéa rédigé comme suit :

« 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. »

Article 3

Est inséré, après l'article 5 de la loi n° 1.430 du 13 juillet 2016, précitée, et avant le Titre V intitulé « *Des traitements automatisés d'informations nominatives mis en œuvre par la Direction de la Sûreté Publique* », un Titre IV bis rédigé comme suit :

« *Titre IV bis - De la vidéosurveillance des lieux accessibles au public.*

Article 5 bis : 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. »

Article 4

Est inséré, après l'article 8 de la loi n° 1.430 du 13 juillet 2016, précitée, et avant le Titre VII intitulé « *De l'interception des correspondances émises par la voie des communications électroniques et de l'accès administratif aux données de connexion* », un Titre VI bis rédigé comme suit :

« *Titre VI bis - De l'utilisation de la vidéoprotection et de la vidéosurveillance des lieux accessibles au public aux fins de détection, de recherche ou d'identification de personnes recherchées ou signalées au moyen de système d'identification biométrique à distance*

Article 8-1 : Le traitement automatisé des images issues des systèmes de vidéoprotection et des systèmes de vidéosurveillance 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 au moyen de système d'identification biométrique à distance aux fins de rechercher ou d'identifier les personnes physiques est interdit.

<u>Article 8-2</u> : Par exception aux dispositions de l'article 8-1, pour la bonne exécution de ses missions de police administrative ou de police judiciaire, le Directeur de la Sûreté Publique met en œuvre, dans le respect des dispositions de la loi n° 1.165 du 23 décembre 1993, modifiée et conformément aux dispositions du présent titre, des traitements automatisés 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 prévues à l'article 8-3, par le recueil en temps réel, sur tout ou partie du territoire, de l'image de personnes capturée par les systèmes de vidéoprotection ou de vidéosurveillance des lieux accessibles au public exploités ou mis à disposition de la Direction de la Sûreté Publique.

Les images issues des systèmes de vidéoprotection ou de vidéosurveillance visés au précédent alinéa sont traitées au moyen d'un système d'identification biométrique à distance destiné à identifier des personnes physiques, en temps réel ou a posteriori, en comparant les données biométriques d'une personne avec celles des personnes inscrites sur les listes d'alerte.

<u>Article 8-3</u> : Afin de permettre les opérations de détection, de recherche et d'identification prévues à l'article 8-2, 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 ;

2°) une liste d'alerte portant sur les personnes recherchées ou signalées au titre de recherches menées pour les besoins d'une enquête préliminaire, d'une enquête de flagrance ou d'une information judiciaire concernant une infraction punie d'une peine supérieure ou égale à un an d'emprisonnement ;

3°) une 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 ;

4°) 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 ;

5°) une liste d'alerte portant sur les personnes recherchées ou signalées au titre de la sécurité des manifestations sportives, culturelles ou récréatives en cas de risque d'atteintes graves à la sécurité des personnes ou des biens ;

6°) une liste d'alerte portant sur les personnes recherchées ou signalées au titre de mesures de refoulement, d'expulsion ou de placement d'office.

Il procède à l'inscription des personnes recherchées ou signalées sur la liste qui correspond, pour chacune d'elles, au motif pour lequel elles sont recherchées ou signalées. Dans l'hypothèse où une personne est recherchée ou signalée pour plusieurs de ces motifs, elle fait l'objet d'une inscription sur chacune des listes afférentes.

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.

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.

Le Directeur de la Sûreté Publique procède à un contrôle mensuel des listes d'alerte visées au premier alinéa ».

<u>Article 8-4</u> : Les opérations de détection, de recherche et d'identification prévues à l'article 8-2 sont mises en œuvre dans les limites de temps et de lieu en rapport avec l'objet de l'inscription de la personne recherchée ou signalée sur les listes d'alerte prévues à l'article 8-3.

<u>Article 8-5</u> : Les données collectées par les systèmes de vidéoprotection ou de vidéosurveillance des lieux accessibles au public sont conservées trente jours.

Durant la période prévue au précédent alinéa, la consultation des données n'ayant pas fait l'objet d'un rapprochement positif par le système d'identification biométrique à distance avec les données des personnes inscrites sur les listes d'alerte prévues à l'article 8-3 est interdite.

La consultation des données n'ayant pas fait l'objet d'un rapprochement positif est toutefois autorisée lorsque celle-ci est justifiée pour les besoins :

1°) d'une enquête préliminaire, d'une enquête de flagrance ou d'une information judiciaire concernant une infraction punie d'une peine supérieure ou égale à un an d'emprisonnement ;

2°) d'enquêtes diligentées dans le cadre de recherches des causes de la mort, de personnes disparues, de disparitions inquiétantes ou de fugues de mineurs ;

3°) de la poursuite des finalités énoncées au deuxième alinéa de l'article 9;

4°) de la coopération judiciaire internationale ;

5°) de la prévention des atteintes graves à la sécurité des biens et des personnes ;

6°) de la prévention des troubles graves à l'ordre public.

<u>Article 8-6</u> : Les données qui ont donné lieu à un rapprochement positif par le système d'identification biométrique à distance avec les données des personnes inscrites sur les listes d'alerte prévues à l'article 8-3 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.

Le rapprochement positif par le système d'identification biométrique à distance avec les données des personnes inscrites sur les listes d'alerte prévues à l'article 8-3 donne lieu au contrôle d'un agent habilité à cet effet.

Un arrêté ministériel détermine les catégories de données dont la durée de conservation est régie par les dispositions du premier alinéa.

<u>Article 8-7</u> : 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.

<u>Article 8-8 :</u> Est puni d'un emprisonnement de six jours à un mois et de l'amende prévue au chiffre 2°) de l'article 26 du Code pénal quiconque met en œuvre un traitement automatisé des images issues des systèmes de vidéoprotection et des systèmes de vidéosurveillance aux fins de rechercher ou d'identifier les personnes physiques dans les lieux accessibles au public au moyen de système d'identification biométrique à distance en méconnaissance des dispositions des articles 8-1 et 8-2. ».