2021-26
14 décembre 2021

PROJET DE LOI, N° 1054,
RELATIVE A LA PROTECTION DES DONNEES PERSONNELLES

EXPOSE DES MOTIFS

Dans un contexte de flux mondialisés, la donnée, notamment à caractère personnel, constitue une valeur économique que les acteurs privés et publics valorisent et mobilisent dans le cadre de leurs activités.

Lesdits acteurs collectent, utilisent et partagent ainsi des données à caractère personnel dont la volumétrie est inédite tandis que les services numériques personnalisés impliquent, pour les personnes physiques, de rendre toujours plus d'informations accessibles les concernant. Ce mouvement – qui transforme à la fois profondément les modèles économiques, les interactions avec les administrations et les rapports sociaux – s'est accompagné d'une prise de conscience plus vive par la société civile des enjeux et des risques associés à une utilisation insuffisamment régulée des données à caractère personnel.

La Principauté avait déjà pris la pleine mesure de cette préoccupation lorsqu'elle a modifié en 2008 la loi n° 1.165 du 23 décembre 1993 relative à la protection des informations nominatives. Cette modification législative a constitué une évolution majeure puisqu'elle a permis d'aligner la réglementation monégasque sur les principes de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, STE n° 108, du Conseil de l'Europe, ci-après désignée Convention 108, permettant ainsi à Monaco d'y adhérer dès 2009. Elle s'est également inscrite dans le contexte du développement mondial de l'économie numérique et dans le respect de l'État de droit qui implique de rechercher le juste équilibre entre l'intérêt général économique, les libertés publiques et les droits fondamentaux.

Treize ans après, force est de constater que le développement toujours plus rapide des technologies, conjugué à la mondialisation des flux, nécessite que la Principauté modernise à nouveau son cadre juridique de protection des données.

Ainsi, en signant le 10 octobre 2018, jour d'ouverture à la signature des États Parties, le Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STCE n° 223) modernisant ladite Convention, la Principauté a témoigné de sa volonté de faire évoluer dans le même sens sa législation de protection des données dans la perspective de la ratification dudit Protocole.

Si la version modernisée de la Convention 108 de 1981, appelée Convention 108+, réaffirme les principes d'origine de protection des données, elle les adapte aux réalités du monde en ligne et introduit de nouveaux principes de transparence, de responsabilité et de respect de la vie privée. À ce titre, les garanties énoncées dans la Convention s'étendent à toute personne physique, indépendamment de sa nationalité et de son lieu de résidence. Elle renforce les pouvoirs des autorités de contrôle et favorise leur coopération sur le plan international.

De portée générale, s'appliquant au secteur public et privé sans distinction, la Convention 108 modernisée institue un mécanisme de suivi par le biais d'un Comité conventionnel lequel n'a plus seulement un rôle consultatif mais un pouvoir d'évaluation et de surveillance, à l'exception des traitements de sécurité nationale et de défense.

La démarche de réforme législative entreprise par la Principauté a ainsi pour ambition de prendre en compte l'évolution des dispositions de la Convention 108+, avec laquelle il s'agit d'être conforme et non pas seulement compatible, et de doter également la Principauté d'un niveau de protection adapté aux nouvelles exigences européennes en matière de protection des données à caractère personnel de sorte à ce qu'une décision dite « *d'adéquation* » soit rendue par la Commission européenne, facilitant par là même les transferts de données avec les pays de l'Union européenne.

Il importe au Gouvernement de rappeler qu'une demande dans ce sens avait été formulée en 2009 par la Principauté qui n'a pu aboutir malgré un avis positif rendu en 2012 par le Groupe 29 ou G29, qui est l'organe chargé de donner un avis sur le niveau d'adéquation du pays tiers à la Commission européenne, et une mise en conformité de la loi intervenue en 2015. En effet, la perspective de l'entrée en vigueur du Règlement Général de Protection des Données (R.G.P.D.) a conduit la Commission européenne à suspendre ses décisions d'adéquation sous l'empire de la directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, destinée à être abrogée, et à ne pas donner suite à la demande d'adéquation de la Principauté.

Dans sa dernière analyse sur les critères de référence pour l'adéquation, le Groupe 29, aujourd'hui dénommé « Comité européen de la protection des données », a précisé que l'objectif pour le pays tiers n'est pas de refléter point par point la législation européenne mais d'établir les exigences essentielles ou fondamentales de cette législation selon la norme définie par la Cour de Justice de l'Union Européenne, à savoir que le « *niveau de protection adéquat* » dans le pays tiers doit être « *substantiellement équivalent* » à celui garanti dans l'Union européenne, et d'ajouter que « *les moyens auxquels ce pays tiers a recours pour assurer un tel niveau de protection peuvent être différents de ceux mis en œuvre au sein de l'Union* ».

Ainsi, le projet de loi a pour ambition de se référer non seulement aux exigences de la Convention 108+ du Conseil de l'Europe mais également au « paquet européen de protection des données » adopté par le Parlement européen et le Conseil le 27 avril 2016 qui se compose :

- du règlement (UE) 2016/679 du 27 avril 2016, dit Règlement Général sur la Protection des Données (R.G.P.D.) relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE;

- de la directive (UE) 2016/680 du 27 avril 2016 relative aux traitements mis en œuvre à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, ci-après désignée directive « *Police-Justice* ».

Dans cette démarche, le Gouvernement s'inscrit également dans le contexte du processus de négociation en cours avec l'Union européenne, le R.G.P.D. faisant partie des textes requis dans l'acquis communautaire.

S'agissant de la directive (UE) 2016/680, précitée, bien qu'elle touche à la souveraineté des États et n'a donc pas vocation à intégrer l'acquis communautaire, le Gouvernement a souhaité prendre en compte ses dispositions afin de renforcer la sécurité juridique applicable aux traitements susvisés, obtenir une reconnaissance d'adéquation au titre de cette directive dans les domaines spécifiques de la coopération judiciaire en matière pénale et de la coopération policière et faciliter par là-même, comme l'intitulé de la directive le prévoit, la libre circulation des données de cette nature avec les pays de l'Union européenne.

De fait, la directive fixe des règles particulières relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel dans les domaines concernés tout en respectant la nature spécifique des activités. Le projet de loi consacre ainsi une section spécifique aux traitements relevant des finalités prévues par la directive.

Bien que la directive ne s'applique pas, tout comme le R.G.P.D., aux activités de sécurité nationale, le projet de loi s'inscrit dans la logique de la Commission européenne qui tient compte dans l'évaluation d'un pays tiers pour l'obtention de l'adéquation de la manière dont ledit pays tiers respecte l'Etat de droit, garantit l'accès à la justice et observe les règles et normes internationales dans le domaine des droits de l'homme, mais également de sa législation générale et sectorielle, y compris la législation sur la sécurité publique, la défense et la sécurité nationale ainsi que l'ordre public et le droit pénal.

Le projet de loi prévoit également, comme le veut la Convention 108+, que les activités de traitement à des fins de sécurité nationale et de défense soient soumises à un contrôle et une supervision indépendants effectifs.

Tenant compte de ces critères, le Gouvernement a choisi d'introduire une section spécifique au sein du projet de loi relatif au contrôle des traitements de sécurité nationale relevant des articles 9 à 15 et 18 de la loi n° 1.430 du 13 juillet 2016 portant diverses mesures relatives à la préservation de la sécurité nationale.

De fait, dans un souci de lisibilité et de cohérence du droit monégasque applicable aux traitements de données à caractère personnel, le Gouvernement a fait le choix de proposer un projet de loi unique relatif à la protection des données et d'abroger la loi n° 1.165 du 23 décembre 1993, modifiée, précitée.

Dans le cadre de sa réflexion, il s'est entouré des avis du Conseil d'Etat, du Haut-Commissaire à la Protection des droits, des libertés et à la médiation et de la Commission de Contrôle des Informations Nominatives (C.C.I.N.).

Ce renouvellement de législation s'accompagne d'une évolution terminologique permettant une interopérabilité juridique plus grande avec les notions relevant de la législation monégasque, d'une part, du droit du Conseil de l'Europe et du droit de l'Union européenne, d'autre part. Ainsi, la notion d'« *informations nominatives* » est abandonnée au profit de la notion de « *données à caractère personnel* » ou de « *données personnelles* ».

Il a également fait le choix de ne pas maintenir l'exercice des droits conférés par la loi n° 1.165 du 23 décembre 1993, modifiée, précitée, aux personnes morales en matière d'accès, de rectification et d'opposition. La pratique ayant démontré que l'exercice de ces droits était extrêmement limité, voire inexistant et source de difficulté pour l'autorité de protection. D'autres pays, comme la France et le Luxembourg ont pris la même décision dès lors que le Règlement européen et la Convention 108 n'ont pas vocation à s'appliquer au traitement de données concernant les personnes morales.

Le R.G.P.D, entré en application le 25 mai 2018, constitue désormais le cadre général et harmonisé applicable à la protection des données à caractère personnel au sein des États membres de l'Union européenne. Les nouvelles règles qu'il comporte consistent à donner aux citoyens plus de contrôle sur leurs données personnelles, à responsabiliser davantage les entreprises tout en réduisant leurs charges déclaratives et à renforcer le rôle des autorités de protection des données. Il s'applique directement à tous les traitements réalisés par un responsable du traitement ou un sous-traitant situé sur le territoire de l'Union européenne. Mais il a également une portée extraterritoriale en concernant directement les pays tiers, et donc Monaco.

Il introduit un certain nombre d'obligations nouvelles, au premier rang desquelles la protection des données dès la conception et par défaut, l'encadrement de la sous-traitance, la réalisation d'une analyse d'impact lorsque les traitements sont susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques et la tenue d'un registre des activités de traitement dans certaines circonstances.

Le R.G.P.D. supprime les formalités déclaratives préalables auprès des autorités de protection, avec le passage d'un système de contrôle *ex ante* par l'autorité de contrôle nationale, par le biais des déclarations et autorisations, à un contrôle *ex post* plus adapté aux évolutions technologiques. Un tel changement de situation repose sur une logique de responsabilisation des acteurs par la mise en place d'un processus de conformité dynamique et continu de protection des données, accompagné d'un renforcement des pouvoirs d'investigation, de régulation et de sanction des autorités de contrôle nationales.

En outre, tant sur le fondement du règlement 2016/679 qu'auparavant sur celui de la directive 95/46/CE, la Commission européenne accepte que des données à caractère personnel puissent être transférées vers un État non-membre de l'Union européenne si le degré de protection de ces données dans cet État tiers est, comme précisé ci-avant, « *substantiellement équivalent* » au standard européen, en prenant une décision d'adéquation.

En l'absence d'une telle décision d'adéquation, le droit européen impose au responsable du traitement ou au sous-traitant de prendre des mesures pour compenser l'insuffisance de protection des données dans le pays tiers à l'Union européenne par l'adoption de garanties appropriées en faveur de la personne concernée. Le présent projet de loi prévoit la mise en place de l'ensemble des garanties susvisées dans le cadre de flux transfrontières hors de la Principauté, vers des pays étrangers, membres ou non de l'Union européenne, et tend à assurer un haut niveau de protection des données.

Le texte projeté introduit donc les obligations nouvelles du R.G.P.D. et les nouveaux droits des personnes, en particulier la portabilité des données et la limitation du traitement. Il renforce également le droit à l'information. Il crée un registre des activités du traitement et prévoit la désignation d'un délégué à la protection des données dans certains cas. Il simplifie les règles auxquelles les acteurs publics et privés traitant des données personnelles sont soumis et supprime le caractère organique d'application de la loi. Les formalités préalables qui s'imposent aujourd'hui à tous les acteurs dans la loi n° 1.165 du 23 décembre 1993, modifiée, précitée, sont supprimées conformément à la logique européenne de responsabilisation du responsable du traitement rappelée ci-avant.

Le Gouvernement a cependant souhaité maintenir des formalités pour certaines catégories de traitement particulièrement sensibles en préférant s'entourer de l'avis de la future autorité de protection.

Est ainsi créée une nouvelle autorité administrative indépendante appelée Autorité de Protection des Données Personnelles (A.P.D.P), qui succède à la Commission de Contrôle des Informations Nominatives (C.C.I.N.) dont l'indépendance et l'effectivité de son activité ne sont plus à démontrer. Cette nouvelle dénomination positionne l'autorité comme étant avant tout « *protectrice* » des personnes physiques lorsque leurs données personnelles font l'objet d'un traitement. Cette autorité sera également chargée de contrôler les traitements relevant de la directive (UE) 2016/680, dite « *police-justice* » comme le préconise le G29 de confier à une même autorité de protection le contrôle des traitements relevant du « *paquet européen de protection des données* ».

À cet égard, comme déjà souligné à l'occasion du vote de la loi n° 1.353 du 4 décembre 2008 modifiant la loi n° 1.165 du 23 décembre 1993, modifiée, précitée, l'article premier de la Constitution – et plus particulièrement la référence qui y est faite aux principes généraux du droit international – fournit une base juridique à la possibilité exceptionnelle de création de telles autorités. Il peut être ainsi rappelé que ces principes incluent la règle de l'effet obligatoire des conventions de telle sorte que la nécessité de donner effet aux engagements internationaux de l'État monégasque devient une exigence constitutionnelle.

Il en résulte que des autorités administratives indépendantes peuvent être créées à Monaco mais uniquement lorsque cela est requis par l'exécution des engagements internationaux de la Principauté. Dans ce cas, elles ne peuvent être investies que des compétences strictement nécessaires à la satisfaction desdits engagements.

En considération de l'engagement de la Principauté à la Convention 108 modernisée, les pouvoirs de la nouvelle autorité de protection des données seront renforcés, en particulier dans le domaine des sanctions.

Ainsi, dans le respect des principes du procès équitable visés à l'article 6 de la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales qui imposent de distinguer le pouvoir d'enquête et de sanction, le présent projet de loi crée une formation restreinte au sein de l'Autorité de Protection des Données Personnelles, chargée de prononcer les sanctions et amendes administratives à l'encontre des responsables du traitement ou des sous-traitants qui ne respecteraient pas les dispositions de la loi.

En sus de la possibilité de pouvoir émettre des recommandations, l'autorité de protection pourra également adopter des lignes directrices destinées à faciliter l'application des règles prévues dans le projet de loi, sans que cela constitue un pouvoir normatif de nature réglementaire, non requis par la Convention 108 modernisée.

S'agissant des traitements relevant des articles 9 à 15 et 18 de la loi n° 1.430 du 13 juillet 2016, précitée, le Gouvernement a fait le choix de s'inscrire dans la possibilité offerte par le R.G.P.D. et la Convention 108+ de créer plusieurs autorités de contrôle indépendantes ou de limiter leur compétence à un secteur donné. Il en est ainsi des traitements liés à des activités de renseignements ou de techniques spéciales d'investigation qui intéressent la sécurité nationale et qui sont régis par les dispositions des articles 9 à 15 et 18 de ladite loi. Le contrôle de ces traitements est confié à la Commission indépendante instituée par l'article 16 de cette loi, dont les missions seront élargies, ci-après désignée Commission de l'article 16.

Le choix opéré par le Gouvernement est guidé par la cohérence. En confiant à cette même autorité indépendante les différents aspects de l'action de l'Etat dans le domaine de la sécurité nationale, à savoir le contrôle de la mise en œuvre des techniques de renseignement, le contrôle de l'exploitation des fichiers de sécurité nationale qui contiennent, notamment, les données collectées au moyen de la mise en œuvre desdites techniques, et enfin l'éventuelle opportunité de déclassifier tout ou partie d'un document ou d'un fichier qui bénéficierait de la protection de l'article 18 de la loi n° 1.430 du 13 juillet 2016, précitée, le Gouvernement privilégie l'efficacité pratique ainsi que la continuité d'action dans le domaine particulier que constitue la sécurité nationale.

Déjà compétente pour apprécier la régularité des mesures individuelles prises en application de la loi n° 1.430, susmentionnée, la Commission de l'article 16 est apparue au Gouvernement l'organe de supervision approprié pour assurer, en toute indépendance, le contrôle de la mise en œuvre des traitements de données personnelles adossé à l'édiction de ces mesures.

Selon les critères du R.G.P.D. et de la Convention 108+, l'autorité de contrôle doit être indépendante, impartiale, publique et disposer de mécanismes indépendants et effectifs de contrôle et de supervision des activités de traitement, y compris à des fins de sécurité nationale et de défense.

Au regard de ces critères, la Commission de l'article 16 remplit les conditions susvisées.

En effet, elle accomplit ses missions en toute indépendance, comme l'indique le deuxième alinéa de l'article 16 de la loi n° 1.430 du 13 juillet 2016, précitée ; elle n'est ni soumise à la tutelle administrative ni au pouvoir hiérarchique et ne reçoit ni ordre ni instruction du Gouvernement ; elle a une composition collégiale de trois membres titulaires et de trois membres suppléants qui ne sont pas révocables.

Sur le plan fonctionnel, et tenant compte de l'avis du Conseil d'État, le présent projet de loi introduit une disposition afin doter ladite Commission d'un budget propre. Elle dispose des moyens matériels et humains nécessaires qui seront renforcés, si besoin, pour accomplir ses nouvelles missions ainsi que d'un secrétariat composé d'un secrétaire titulaire et d'un suppléant désignés par le Secrétaire d'État à la Justice, Directeur des Services Judiciaires parmi les personnels administratifs.

Par ailleurs, son impartialité ne peut être mise en doute : compte tenu de sa composition collégiale et du mode de désignation de ses membres, elle apparaît objectivement impartiale et son caractère public est incontestable. Afin de renforcer ce critère d'indépendance, le projet de loi prévoit de porter la durée du mandat des membres de un à cinq ans.

Enfin, la Commission dispose d'un pouvoir de contrôle et de recommandation qu'elle exerce de manière effective et de sa propre initiative dans les domaines de ses compétences.

En conclusion, au regard de la Convention 108+ mais également des critères du G29 dégagés de la jurisprudence tant de la Cour de Justice de l'Union européenne que de la Cour européenne des droits de l'Homme, la Commission de l'article 16 présente tous les attributs permettant un contrôle indépendant.

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 présent projet de loi est divisé en dix Chapitres :

- Chapitre I – Dispositions générales
- Chapitre II – Principes relatifs à la qualité des données et aux conditions de licéité des traitements de données à caractère personnel
- Chapitre III – Droits de la personne concernée
- Chapitre IV – Obligations incombant au responsable du traitement et au sous-traitant
- Chapitre V – De l'Autorité de protection des données personnelles
- Chapitre VI – Traitements soumis à formalités préalables
- Chapitre VII – Dispositions particulières à certains traitements
- Chapitres VIII – Transfert de données à caractère personnel
- Chapitre IX – Compétences juridictionnelles, sanctions pénales et droit à réparation
- Chapitre X – Dispositions finales

Le Chapitre I contient trois articles relatifs aux principes de la loi, aux définitions et au champ d'application.

L'article premier confirme, dans son premier alinéa, le principe de protection des libertés et droits fondamentaux visés au titre III de la Constitution à l'égard du traitement de données à caractère personnel, quel que soit le procédé utilisé, automatisé ou non automatisé. Inscrit sous forme de principe général dans la loi n° 1.165 du 23 décembre 1993, modifiée, précitée, l'article premier le réitère en adoptant la terminologie de « *données à caractère personnel* » qui est celle généralement retenue par les législations étrangères, par l'Union européenne et par le Conseil de l'Europe et remplace celle « *d'informations nominatives* ».

Le second alinéa consiste à préciser ce que vise à garantir le projet de loi, à savoir protéger les personnes physiques à l'égard des traitements qui peuvent être faits de leurs données personnelles et garantir que leurs droits s'exerceront selon les modalités définies par la loi.

Le projet de loi comporte 23 définitions présentées par ordre alphabétique à l'article 2. Inspirées dans leur grande majorité du Règlement européen et de la Convention 108 modernisée du Conseil de l'Europe, ces définitions sont pour la plupart nouvelles par rapport à celles de la loi n° 1.165, précitée, qui n'en compte que cinq (information nominative, traitement, responsable du traitement, destinataire et personne concernée).

Lesdites définitions contribuent à une meilleure compréhension et application de la loi. A partir du moment où les données doivent être traitées de manière loyale, licite et légitime, il importe que les fondements au titre desquels ces données peuvent être traitées soient définis de façon suffisamment claire.

Les commentaires suivants peuvent être formulés sur des notions clefs :

Concernant le « *chiffrement* », le Gouvernement a souhaité l'introduire dans le projet de loi afin de clarifier cette notion technique bien que ne figurant pas au titre des définitions européennes. Le chiffrement permet de rendre les informations d'un document illisibles afin d'en garder la confidentialité. Il s'agit d'un processus réversible qui ne fait que masquer les données à des utilisateurs qui ne sont pas habilités à les voir. Il est donc toujours possible de retrouver leur valeur initiale grâce à une clé. Cette clé, qui est un algorithme de déchiffrement, va permettre de verrouiller et déverrouiller le chiffrage des informations.

S'agissant du « *consentement* », qui s'entend comme étant celui de la personne concernée par le traitement, celui-ci doit être libre, spécifique, éclairé et non équivoque.

Le consentement n'est donné « *librement* » que si la personne concernée n'est pas dans une relation de déséquilibre manifeste avec le responsable du traitement, qu'elle peut refuser ou retirer son consentement sans subir de préjudice. Il est « *spécifique* » car le consentement de la personne concernée doit être donné en lien avec une ou plusieurs finalités spécifiques du traitement et la personne concernée doit avoir un choix concernant chacune de ces finalités. Il ne peut être considéré comme « *éclairé* » si la personne concernée ne connaît pas l'identité du responsable du traitement, par exemple, ou si la demande de consentement n'est pas formulée en des termes simples et compréhensibles. Enfin, il doit être « *non équivoque* », c'est-à-dire exprimé par un acte positif clair, par écrit, par voie électronique ou à l'oral sous réserve d'en rapporter la preuve.

Dans certains cas, comme pour le traitement de données sensibles, le consentement doit être explicite, c'est-à-dire obtenu au moyen d'une déclaration expresse de la part de la personne concernée (case particulière à cocher, déclaration écrite…). L'article 6 du projet de loi précise les conditions particulières applicables au consentement.

Sont également définies les « *données à caractère personnel* » ou « *données personnelles* ». La définition se rapproche sensiblement de celle qui existe dans la loi n° 1.165 du 23 décembre 1993, modifiée, précitée sous l'expression d'« *informations nominatives* ». Comme précisé ci-avant, il est apparu plus efficient au Gouvernement d'adopter la terminologie communément employée au niveau européen de données personnelles ou à caractère personnel. Cette notion de « *données* » est plus adaptée au développement des technologies d'identification par le biais de moteurs de recherche ou de logiciels spécifiques, comme par exemple la reconnaissance vocale, qui permettent d'identifier une personne physique, directement ou indirectement. La définition a été complétée par l'introduction des données génétiques et des données de localisation.

La définition relative aux « *données concernant la santé* » est celle retenue par le Conseil de l'Europe, dans sa Recommandation du 27 mars 2019 en matière de protection des données relatives à la santé. Elle s'entend comme relative à l'état de santé passé, actuel et futur de la personne concernée. Bien que les données de santé ne soient pas directement traitées dans le projet de loi, il a été jugé opportun d'introduire cette définition dès lors qu'il s'agit de données sensibles et qu'elles sont concernées à ce titre.

Le projet de loi définit les « *données génétiques* » et les « *données biométriques* » qui figurent également au titre des données sensibles. Le projet de loi reprend les définitions européennes.

Ainsi, la biométrie se réfère aux caractéristiques physiques mais également aux caractéristiques comportementales d'un individu, comme par exemple la gestuelle ou la démarche. Elle vise également les images faciales. Toutefois, celles-ci ne constituent pas nécessairement des données biométriques. En effet, une photographie n'est considérée comme une donnée biométrique que lorsqu'elle est traitée pour une finalité d'identification ou d'authentification unique d'une personne physique.

Ainsi, un enregistrement de voix constitue une donnée biométrique uniquement si cet enregistrement est destiné à identifier une personne unique ; cela ne sera pas le cas lorsque l'enregistrement vocal a pour finalité d'améliorer le service qualité d'une entreprise sans identification de la personne.

Les données génétiques sont relatives à des caractéristiques héréditaires et sont notamment utilisées dans le domaine de la santé. Elles peuvent également être utilisées pour une finalité d'identification d'une personne par le biais de ses empreintes génétiques.

S'agissant des « *données sensibles* », intitulées « *catégories particulières de données* » dans les textes européens, le Gouvernement a fait le choix de conserver cette expression, qui est celle utilisée dans la loi n° 1.165 précitée, et de l'intégrer dans les définitions pour plus de clarté. Ainsi, les données sensibles sont celles qui révèlent, directement ou indirectement, des opinions ou des appartenances politiques, raciales ou ethniques, religieuses, philosophiques ou syndicales, mais également des données génétiques, des données biométriques dès lors qu'elles permettent d'identifier une personne physique de manière unique ou des données concernant la santé, la vie sexuelle ou l'orientation sexuelle d'une personne physique.

Ne figurent plus dans la nouvelle définition les données relatives aux mœurs et aux mesures à caractère social, qui ne sont pas considérées comme des données sensibles au niveau européen et dont le libellé trop général ne permet pas une juste appréciation ni de cerner précisément les données auxquelles s'appliquent ces mesures.

Une nouvelle définition porte sur la « *limitation du traitement* ». Il s'agit d'un moyen technique de marquage destiné à suspendre l'utilisation ultérieure des données sans pour autant les effacer. Une limitation peut être sollicitée le temps que le responsable du traitement vérifie l'exactitude des données qu'il détient sur une personne.

Le « *profilage* » est également défini comme étant toute forme de traitement permettant d'évaluer certains aspects personnels d'une personne, notamment ses préférences de consommation dans différents domaines, culturels, sportifs, alimentaires ou encore ses sensibilités politiques. Le projet de loi encadre le recours au profilage.

La « *pseudonymisation* » est également définie. Ce procédé fait partie des mesures susceptibles d'être adoptées notamment au titre des garanties appropriées que doit prendre le responsable du traitement dans certaines situations mais également en matière de sécurité des données.

Contrairement à l'anonymisation qui neutralise irréversiblement les données des lors qu'elles ne permettent pas ou plus d'identifier, directement ou indirectement une personne physique, la pseudonymisation permet toujours d'identifier un individu grâce à ses données personnelles car elle consiste simplement à remplacer les données directement identifiantes (nom, prénom…) par des données indirectement identifiantes (alias, numéro séquentiel…). Pour autant, les données pseudonymisées demeurent juridiquement des données à caractère personnel.

Une nouvelle définition concerne les « *règles d'entreprises contraignantes* » communément appelées BCR (*Binding Corporate Rules)*. Ces règles sont un outil d'encadrement des transferts de données vers les pays tiers qui permettent à des groupes d'entreprises d'encadrer juridiquement et de sécuriser leurs transferts de données.

La définition du « *responsable du traitement* », qui apparait déjà dans la loi n° 1.165 du 23 décembre 1993, modifiée, précitée est légèrement modifiée pour la faire correspondre plus précisément aux standards européens. Il s'agit de la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui détermine seul ou conjointement avec d'autres, les finalités et les moyens du traitement. Au sens de la Convention 108+, comme du R.G.P.D. ou de la Directive, le responsable du traitement est la personne ou l'organe qui dispose du pouvoir de décision à l'égard des finalités et des moyens du traitement de données.

La définition relative au « *traitement* » est complétée par rapport à celle de la loi n° 1.165, précitée. La notion de « *traitement* » est un concept exhaustif qui recouvre toute une série d'opérations (collecte, enregistrement, communication, extraction…) effectuées sur des données à caractère personnel à l'aide de procédés automatisés ou non. Ainsi, s'agissant d'un site Internet, la diffusion de données personnelles s'analyse comme une diffusion d'informations et constitue un traitement.

De même, la mise en relation de deux traitements de données à caractère personnel distincts ayant des finalités différentes et permettant l'analyse comparative de deux fichiers constitue un « *rapprochement d'informations* » et donc un traitement. Elle intègre également, par référence à la Convention 108+ du Conseil de l'Europe, la notion « *d'opérations logiques ou arithmétiques* » qui permet d'effectuer des opérations à partir de données d'entrée (data input) et de produire des résultats désignés sous le terme de sortie (output).

L'article 3 est relatif aux champs d'application matériel et territorial du projet de loi. Il reprend, du point de vue de la Principauté, le mécanisme résultant de l'article 3 du R.G.P.D. qui étend les règles de protection des données de l'Union aux responsables du traitement établis en-dehors de son territoire. Cette extension impose aux responsables du traitement de données et aux sous-traitants établis hors de l'Union de respecter les obligations en matière de protection des données européennes lorsqu'ils traitent les données de sujets résidant dans l'Union à des fins spécifiques.

Les nouveaux critères visés au chiffre 1 confèrent donc au projet de loi une portée territoriale et extraterritoriale. Leur application a notamment pour conséquence de déplacer la question de la localisation des moyens de traitement vers celle du lieu de résidence ou de séjour des personnes concernées.

Le second tiret du chiffre 1 permet d'appliquer le projet de loi aux situations dans lesquelles le responsable du traitement ou le sous-traitant ne sont pas établis sur le territoire monégasque mais réalisent des activités de traitement qui sont liées soit à l'offre de biens ou de services à destination de personnes physiques se trouvant à Monaco, soit au suivi du comportement de ces mêmes personnes.

À titre d'exemple, le projet de loi a ainsi vocation à s'appliquer à la situation dans laquelle un responsable du traitement, ou un sous-traitant, situé à l'étranger ciblerait, grâce à son site Internet, les consommateurs à Monaco pour leur proposer des biens et des services en leur permettant de passer leur commande en français, de la régler en euros et de se faire livrer à Monaco.

De même, il pourrait également s'appliquer à la situation dans laquelle un responsable du traitement, ou un sous-traitant, établi à l'étranger suivrait les internautes établis en Principauté, par exemple au moyen de cookies et traceurs, pour leur adresser ensuite de la publicité ciblée.

Cette disposition permet ainsi de protéger uniformément les personnes physiques dont les données sont traitées, que le responsable du traitement et le sous-traitant soient ou non établis sur le territoire monégasque.

Le chiffre 2 introduit deux dérogations au champ d'application de la loi. La première dérogation concerne l'exclusion des traitements relatifs aux activités personnelles et domestiques qui figure déjà à l'article 24-2 de la loi n° 1.165 du 23 décembre 1993, modifiée, précitée, et qui est prévue à l'article 2 du R.G.P.D. et à l'article 3 de la Convention 108+. On entend par activités personnelles et domestiques des activités qui n'ont aucun aspect professionnel, commercial ou associatif, qui n'ont pas d'impact significatif sur la sphère personnelle d'autrui. Il peut s'agir du stockage de photos de famille ou de photos privées sur un ordinateur ou d'une liste de coordonnées d'amis ou de membres de la famille. Cette exclusion a pour objet de ne pas imposer des obligations déraisonnables à de tels traitements qui sont liés à la vie privée.

La seconde dérogation concerne les copies temporaires réalisées dans le cadre des activités techniques de transmission et de fourniture d'accès à un réseau numérique. Elle prend en compte les spécificités d'Internet et celles des réseaux numériques et, ainsi, les opérations d'optimisation et de régulation du trafic. Prévue dans la loi de protection des données en France, cette dérogation est intégrée dans le projet de loi pour des raisons de cohérence et d'efficience dans le domaine des télécommunications.

Le Chapitre II comporte 5 articles relatifs aux principes et conditions de licéité applicables aux traitements de données.

L'article 4 expose les principes essentiels constituant aujourd'hui le fondement du droit européen en matière de protection des données à caractère personnel. Déjà consacrés dans la loi n° 1.165 du 23 décembre 1993, modifiée, précitée ces principes sont actualisés et complétés par référence au R.G.P.D. et à la Convention 108+.

En premier lieu, sont visées au chiffre 1, les caractéristiques de loyauté, de licéité et de transparence auxquelles doit répondre tout traitement de données à caractère personnel.

Le chiffre 2 introduit deux novations : tout d'abord, il offre la possibilité de collecter des données à caractère personnel non plus pour une finalité unique par traitement mais pour plusieurs finalités dès lors qu'elles sont déterminées, explicites et légitimes et qu'elles ne sont pas traitées ultérieurement de manière incompatible. Il en est ainsi, par exemple, pour le service marketing d'une entreprise qui pourra collecter des données ayant vocation à être traitées à des fins de prospection commerciale mais également pour la réalisation d'évènements promotionnels. La seconde novation porte sur la possibilité de réaliser un traitement ultérieur de données à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques dès lors qu'un tel traitement est considéré *a priori* compatible avec la finalité initiale de la collecte, comme le prévoit le Règlement européen.

Cette compatibilité n'est cependant pas prévue par la directive (UE) 2016/680, ce qui explique l'exception introduite pour les traitements visés à l'article 61 et pour les traitements de sécurité nationale visés à l'article 87.

Au sens du R.G.P.D., les traitements à des fins archivistiques dans l'intérêt public sont ceux qui sont mis en œuvre par une autorité publique ou privée ayant une obligation légale de collecte, de conservation et de communication ou de diffusion d'archives qui sont à conserver à titre définitif dans l'intérêt public général. Pour ce qui concerne Monaco, il s'agit notamment du Service central des archives et de la documentation administrative qui gère les archives définitives produites ou reçues par les services exécutifs de l'Etat dans l'exercice de leur activité et la Mairie qui gère notamment les archives du service de l'état-civil. Ne sont pas concernées les archives des entités privées dans la mesure où les personnes ou organismes en cause n'ont pas d'obligation légale de collecte, de conservation, de traitement et de communication de leurs archives. Toutefois, lorsque le traitement a pour finalité la recherche historique, les archives issues de ces entités privées peuvent revêtir un caractère d'intérêt public. Des dispositions spécifiques applicables à ces catégories de traitements sont prévues à l'article 78 du présent projet de loi.

Le chiffre 3 prévoit que les données doivent être adéquates, pertinentes et « *limitées* » à ce qui est nécessaire au regard de la finalité du traitement. Il s'agit du principe de « *minimisation* » des données qui doit conduire le responsable du traitement à ce que les données collectées ne soient plus « *non excessives* » comme le prévoit la loi en vigueur mais « *limitées* » à la réalisation de ses objectifs.

Le chiffre 4 porte sur l'exactitude des données et leur mise à jour. Le responsable du traitement doit prendre des mesures raisonnables pour y parvenir, c'est-à-dire qui ne nécessitent pas des efforts disproportionnés.

Le chiffre 5 précise que les données doivent être conservées pour une période limitée à celle nécessaire à la réalisation des finalités du traitement. Toutefois, comme le permet le R.G.P.D., la possibilité de conserver plus longtemps les données dans le traitement initial au-delà de la durée de conservation est autorisée à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques. Le projet de loi prévoit qu'à la fin de cette période de conservation, qui correspond habituellement à la durée d'utilité administrative, un choix puisse être opéré par le responsable du traitement dans les conditions prévues par l'Ordonnance Souveraine n° 8.569 du 25 mars 2021 relative aux archives d'intérêt public. Ce choix peut aboutir à une conservation partielle ou intégrale des données issues d'un traitement, en fonction des cas et de l'intérêt de ces données à des fins archivistiques, à des fins de recherche scientifique ou historique ou à des fins statistiques.

Le chiffre 6 introduit une nouvelle caractéristique en ce qu'il prévoit que le responsable du traitement doit prendre les mesures techniques et organisationnelles nécessaires afin de garantir l'intégrité et la confidentialité des données.

L'article 5 est également un article central en terme de protection des données à caractère personnel car il concerne la licéité du traitement. Le premier alinéa de l'article énonce les six fondements possibles de licéité sur lesquels doit reposer tout traitement de données à caractère personnel. Le responsable du traitement doit satisfaire au moins à l'un d'entre eux.

Lesdits fondements sont : le consentement, le respect d'une obligation légale, l'exécution d'un contrat, la sauvegarde des intérêts vitaux de la personne concernée, l'existence d'un motif d'intérêt public et enfin la réalisation d'un intérêt légitime, lequel pourrait par exemple être réalisé lorsqu'il existe une relation pertinente et appropriée entre la personne concernée et le responsable du traitement (la personne concernée est un client du responsable du traitement ou est à son service, par exemple). En tout état de cause, l'existence d'un intérêt légitime doit tenir compte des intérêts et droits fondamentaux de la personne concernée.

D'une manière générale, l'intérêt légitime ne s'applique pas aux traitements effectués par les autorités publiques dans le cadre de leurs missions dès lors qu'est prévu par ailleurs le fondement du motif d'intérêt public. Cependant, le Groupe 29 a admis que l'intérêt légitime pourrait constituer une base juridique pertinente et être invoqué par une personne publique indépendamment de la mission de service public et de l'activité du traitement. Il peut en être ainsi notamment pour assurer la bonne gestion ou le fonctionnement de l'organisme public ou pour des activités n'entrant pas dans le cadre de la mission de service public. À titre d'exemple, peuvent être citées des entités telles que la Compagnie monégasque des autobus ou Monaco Télécom qui invoquent l'intérêt public dans le cadre des activités de leur concession, mais qui peuvent également se prévaloir de l'intérêt légitime au titre de leurs activités commerciales privées.

A l'instar de ce que prévoit le R.G.P.D, lorsque le traitement est mis en œuvre pour la réalisation d'un motif d'intérêt public, un même fondement légal peut suffire pour plusieurs opérations de traitement justifiées par le respect d'une obligation légale à laquelle le responsable du traitement est soumis, y compris à des fins de santé.

De même, le R.G.P.D. précise que lorsqu'il est fait référence à une base juridique ou à une mesure législative, cela ne signifie pas nécessairement que l'adoption d'un acte législatif par un parlement est exigée. Il importe que cette base juridique ou cette mesure législative soit claire et précise et son application prévisible pour les justiciables, conformément à la jurisprudence de la Cour de Justice de l'Union européenne et de la Cour européenne des droits de l'homme.

Une nouvelle condition de licéité du traitement apparait par rapport à celles énoncées dans la loi n° 1.165 du 23 décembre 1993, modifiée, précitée. Il s'agit de l'intérêt vital de la personne concernée. Il en est ainsi, par exemple, lorsque le traitement est nécessaire à des fins humanitaires.

Le second alinéa de l'article 5 concerne le traitement ultérieur de données à caractère personnel pour d'autres finalités que celles pour lesquelles les données ont été initialement collectées. Comme le prévoit le R.G.P.D, aucune base juridique distincte de celle qui a permis la collecte des données à caractère personnel n'est requise lorsque le traitement est compatible avec les finalités initiales comme c'est le cas pour un traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques.

Il précise également les critères que doit prendre en compte le responsable du traitement pour déterminer si les finalités ultérieures sont compatibles avec celles pour lesquelles il a collecté les données. Lorsque le traitement est fondé sur le consentement ou sur un motif d'intérêt public, le responsable du traitement n'est pas tenu par le principe de compatibilité des finalités. Il pourra s'agir par exemple de révéler l'existence d'éventuelles infractions pénales ou de menaces pour la sécurité publique et de transmettre à une autorité compétente les données à caractère personnel à moins qu'une telle transmission soit incompatible avec une obligation de confidentialité légale, professionnelle ou toute autre obligation de confidentialité contraignante.

L'article 6 détermine les conditions spécifiques applicables en matière de consentement.

Ainsi, la personne concernée doit pouvoir manifester son accord au traitement de ses données personnelles de façon libre, spécifique, éclairée et univoque, par exemple au moyen d'une déclaration qui peut être écrite, y compris par voie électronique, ou orale. La déclaration doit être rédigée en des termes clairs et simples, montrant que la personne est consciente du consentement donné et de sa portée. Il peut s'agir également d'une case à cocher lors de la consultation d'un site internet indiquant clairement que la personne concernée accepte le traitement proposé de ses données à caractère personnel.

Le consentement donné doit couvrir l'ensemble des activités de traitement qui poursuivent la ou les mêmes finalités. Lorsque le traitement a plusieurs finalités, la personne concernée doit pouvoir choisir de donner ou non son consentement distinctement pour chacune d'elles. Les cases à cocher pré-validées ne peuvent constituer un consentement.

Des dispositions spécifiques au recueil du consentement des mineurs sont prévues afin d'assurer un niveau de protection correspondant à leur vulnérabilité. L'information qui leur est donnée est adaptée et, avant l'âge de 15 ans, ils ne peuvent consentir qu'avec l'action conjointe du titulaire de l'autorité parentale.

Comme le prévoit déjà la loi n° 1.165 du 23 décembre 1993, modifiée, précitée, le quatrième alinéa de l'article 6 vise à créer les conditions d'une confiance dans le développement du commerce électronique et, à ce titre, il conserve la nécessité d'un consentement « *exprès* », lequel se matérialise par un double consentement, c'est-à-dire le consentement initial et sa confirmation (via un double clic par exemple).

L'article 7 est relatif aux données qui, par nature, sont particulièrement sensibles du point de vue des libertés et des droits fondamentaux. Le présent projet, comme le fait déjà la loi n° 1.165 du 23 décembre 1993, modifiée, précitée, pose le principe d'interdiction de traiter ces données. Il peut cependant exister des situations dérogatoires qui légitiment le traitement de données sensibles. Le projet de loi identifie 12 situations de traitements pour lesquels des données sensibles peuvent être collectées, par référence à ce que prévoient les standards européens. Les dérogations visées aux chiffres 1, 3, 4, 5, 6 et 7 sont identiques à celles figurant dans la loi n° 1.165, sous réserve de quelques ajustements rédactionnels. Il s'agit notamment de traitements basés sur le consentement explicite de la personne concernée ou portant sur des données manifestement rendues publiques ou encore justifiés par des motifs d'intérêt public important. Par l'ajout de l'adjectif « *important* », le projet de loi se conforme à la formulation plus restrictive du Règlement européen.

Les nouvelles finalités introduites dans le projet de loi sont les suivantes :

- la sauvegarde des intérêts vitaux de la personne concernée lorsque celle-ci se trouve dans l'incapacité de donner son consentement notamment du fait de l'altération de ses facultés personnelles ;

- l’archivage dans l’intérêt public, mis en œuvre par les services ayant une obligation légale de collecte, de conservation et de communication d’archives définitives ou concernant des archives provenant d’entités privées revêtant un caractère d’intérêt public, et à des fins de recherche scientifique ou historique ou statistique. Comme précisé ci-avant, il s’agit dans le domaine de l’archivage, d’assurer la conservation permanente de documents qui, en raison principalement de leur intérêt historique ou patrimonial, ont vocation à être conservés sans limitation de durée et d'assurer la sauvegarde de la mémoire ;

- l’utilisation de données biométriques par les employeurs dès lors qu’elles sont strictement nécessaires aux contrôles de l’accès aux lieux de travail par exemple. Ces nouvelles finalités permettent de concilier l’utilisation des nouvelles technologies dans le monde du travail tout en respectant les droits et libertés des personnes concernées ;

- l’exécution d’obligations incombant au responsable du traitement en matière de droit du travail, de sécurité sociale, de protection sociale.

Pour les traitements relevant de ces finalités, des dérogations à l'interdiction de traiter des données sensibles peuvent être appliquées, sous réserve de garanties appropriées et lorsque l'intérêt public le commande, pour le traitement des données à caractère personnel dans le domaine du droit du travail et du droit de la protection sociale, y compris les retraites, et à des fins de sécurité, de surveillance et d'alerte sanitaire, de prévention ou de contrôle de maladies transmissibles et d'autres menaces graves pour la santé. Ces dérogations sont possibles à des fins de santé, y compris la santé publique et pour la gestion des services de soins de santé et de services dans le régime d'assurance-maladie, ou à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques.

En matière de statistiques, le projet de loi habilite l’Institut Monégasque de la Statistique et des Études Économiques à collecter et traiter des données sensibles dans le cadre de ses missions, selon des modalités en vigueur par la réglementation monégasque en matière de statistiques.

Enfin, lorsque le traitement est mis en œuvre pour les finalités prévues par la Directive (UE) 2016/680, pour les finalités de sécurité nationale visées à l'article 87 ou encore lorsqu'il porte sur des données génétiques ou biométriques permettant l'identification d'une personne unique, le traitement de données sensibles n'est possible que s'il est effectué par une autorité administrative ou judiciaire compétente agissant dans le cadre des missions qui leur sont légalement conférées.

Le dernier alinéa de l'article 7 porte sur les garanties appropriées. D'une manière générale, le responsable du traitement doit adopter des mesures techniques et organisationnelles de façon à garantir un niveau de sécurité adapté aux risques comme le prévoit l'article 28 du projet de loi. En plus de ces mesures, le traitement de données sensibles doit être assorti de garanties appropriées qui sont propres à chaque catégorie de traitement en fonction des modalités de sa mise en œuvre et de ses spécificités. Ces garanties doivent permettre de prévenir les risques pour les intérêts, droits et libertés fondamentales de la personne concernée, notamment un risque de discrimination.

Certaines d'entre elles sont précisées dans le cadre des dérogations prévues par la loi. Ainsi, à titre d'illustration, le fait que le traitement de médecine préventive visé au chiffre 7 soit effectué par un professionnel de la santé soumis au secret professionnel constitue une garantie appropriée. De même, les avis de l'autorité de protection constituent des garanties appropriées lorsqu'elle est consultée pour la mise en œuvre de traitements visés au chiffre 12.

Dans les cas visés aux chiffres 2, 6 et 8 à 11, le responsable du traitement adopte les garanties appropriées les plus adaptées aux risques, qui peuvent être cumulatives. Ces garanties peuvent se matérialiser de la manière suivante : le consentement explicite de la personne concernée, une disposition législative ou réglementaire couvrant le but poursuivi et les modalités du traitement, le secret professionnel, l'adoption de mesures faisant suite à une analyse de risque ou à des recommandations de l'autorité de protection ou encore une mesure de sécurité particulière d'ordre organisationnel ou technique, comme le chiffrement des données, par exemple.

L'article 8 réitère le principe, déjà prévu dans la loi n° 1.165, de l'interdiction de connexion du casier judiciaire avec tout autre fichier de traitement de données à caractère personnel détenu par une personne quelconque ou par un service ne dépendant pas de la Direction des Services Judiciaires.

Le Chapitre III comporte 12 articles relatifs aux droits des personnes physiques. Certains droits sont différents dans le cadre des traitements mis en œuvre à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces, comme le prévoit la directive (UE) 2016/680, ou encore pour les traitements relevant des articles 9 à 15 et 18 de la loi n° 1.430 du 13 juillet 2016, précitée. Des dérogations à l'exercice de ces droits sont ainsi prévues à certains articles, dans le respect des dispositions de l'article 11 de la Convention 108+ et de l'article 23 du R.G.P.D.

Les articles 9 et 10 se rattachent au principe de transparence.

L'article 9 pose l'obligation pour le responsable du traitement de prendre les mesures appropriées pour fournir toute information à la personne concernée et faciliter l'exercice de ses droits.

L'article 10 porte sur le droit à l'information qui est renforcé. L'exercice de ce droit suppose une attitude proactive du responsable du traitement. Il doit communiquer à la personne concernée son identité et ses coordonnées, le fondement juridique du traitement et ses finalités ainsi que d'autres informations précisément listées. Il doit également préciser s'il a l'intention d'effectuer un transfert des données et, dans l'affirmative, les dispositions mises en œuvre selon que le pays ou l'organisme destinataire dispose ou pas d'une protection adéquate.

Certaines dérogations à l'exercice du droit d'information peuvent s'appliquer lorsque cette information se révèle impossible ou implique des efforts disproportionnés du responsable du traitement. Tel est notamment le cas lorsque la personne concernée n'est pas directement identifiable ou qu'il n'existe aucun moyen de la contacter.

Le responsable du traitement peut utiliser tous les moyens disponibles, raisonnables et économiquement abordables pour informer les personnes concernées, de façon collective (site web, information publique) ou individuelle.

Une exception est prévue à l'exercice des droits visés aux articles 9 et 10 concernant les traitements de sécurité nationale portant sur les articles 9 à 15 et 18 de la loi n° 1.430 précitée, visés à la section VI du chapitre VII. En effet, l'exercice de ses droits, s'ils étaient envisagés, serait de nature à rendre impossible ou nuire gravement à la réalisation des finalités de ces traitements qui, par définition, doivent rester confidentiels à l'égard de la personne concernée pour des raisons de sécurité nationale.

Les articles 11, 12 et 13 concernent le droit d'accès, le droit de rectification et le droit à l'effacement.

Ces droits ont été introduits dans la loi n° 1.165 du 23 décembre 1993, modifiée, précitée. Le droit d'accès est le premier des droits car il conditionne l'exercice des autres, en particulier le droit de rectification, le droit d'effacement ou le droit d'opposition.

L'article 11 relatif au droit d'accès permet à la personne concernée d'obtenir auprès du responsable du traitement confirmation que ses données ont été traitées, et dans l'affirmative, leur communication sous une forme lisible et compréhensible. Ce droit peut être exercé par voie électronique lorsque les données à caractère personnel sont traitées électroniquement.

Il énonce la liste des informations que la personne concernée peut obtenir auprès du responsable du traitement lorsqu'elle en fait la demande. Parmi ces informations, figurent notamment l'existence ou non d'une décision individuelle automatisée ainsi que le raisonnement qui sous-tend le traitement. Le responsable du traitement doit également fournir l'information relative à l'existence d'un transfert vers un pays ne bénéficiant pas de la protection adéquate ou ne présentant pas un niveau approprié de protection au regard des dispositions de la présente loi.

Il est également tenu d'apporter toute information disponible sur la source des données qui ont pu être collectées par d'autres personnes permettant ainsi à la personne concernée de vérifier qu'elle a bien donné son consentement.

L'article 12 prévoit que lorsque les données s'avèrent inexactes ou incomplètes, la personne concernée peut demander, sur justificatifs, à ce qu'elles soient rectifiées ou complétées.

L'article 13 donne la possibilité, pour la personne concernée, d'obtenir du responsable du traitement, dans des cas précisément définis, que ses données soient effacées, que celles-ci soient publiques ou non. Il en est ainsi notamment lorsque la personne a retiré son consentement ou bien lorsque les données ont été collectées auprès d'enfants mineurs de moins de 15 ans dans le cadre d'une offre de service sur internet.

Dans certaines circonstances, le droit à l'effacement ne s'applique pas, par exemple, lorsque le traitement répond à une obligation légale ou à une mission d'intérêt général effectuée par une personne morale de droit privé qui en est investie ou concessionnaire d'un service public ou encore si le traitement est nécessaire pour exercer une mission relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement. Il en est ainsi par exemple du Centre Hospitalier Princesse Grace, lorsqu'il met en œuvre un traitement dans le domaine de la santé publique.

Par ailleurs, dans un souci de renforcement du droit à l'oubli numérique, le projet de loi introduit une disposition prévoyant l'obligation pour le responsable du traitement qui a rendu les données à caractère personnel publiques de prendre des mesures raisonnables, compte tenu des technologies disponibles et des moyens dont il dispose, pour que les données ne soient plus publiquement accessibles et d' informer les autres responsables du traitement traitant ces données qu'il convient d'effacer tout lien vers ces données ou toute copie ou reproduction de celles-ci.

L'article 14 introduit un nouveau droit qui permet à la personne concernée d'obtenir la limitation du traitement de ses données.

In concreto, pour assurer l'effectivité de la limitation d'un traitement, le responsable du traitement peut utiliser différentes méthodes telles que le déplacement des données concernées vers un autre système de traitement, le retrait des données publiées sur un site Internet ou le blocage de l'accès des utilisateurs à ces données.

La limitation peut également être techniquement assurée de manière à ce que les données ne puissent être ni traitées ni modifiées et qu'elles soient identifiées comme appartenant à un traitement faisant l'objet d'une limitation.

Ce droit n'est pas applicable aux traitements visés aux articles 61 et 87 pour lesquels un droit de rectification et un droit d'effacement sont spécifiquement prévus.

L'article 15 prévoit que le responsable du traitement notifie à chaque destinataire auquel les données ont été communiquées les rectifications, limitations ou effacements qui ont été effectués à l'occasion du traitement à moins qu'une telle communication se révèle impossible ou exige des efforts disproportionnés.

L'article 16 est relatif au droit d'opposition. Ce droit s'exerce différemment selon les finalités du traitement.

Ainsi, dans le cadre de la prospection commerciale, la personne concernée a le droit de s'opposer à tout moment au traitement de ses données et n'a pas à justifier l'exercice de son droit d'opposition auprès du responsable du traitement qui sera tenu d'y faire droit.

Lorsque le traitement est fondé par un motif d'intérêt public ou par la réalisation d'un intérêt légitime, le droit d'opposition au traitement peut s'exercer si la personne invoque des raisons tenant à sa situation particulière à moins que l'intérêt légitime du responsable du traitement ne prévale sur les intérêts et droits et libertés de la personne concernée et justifie la poursuite du traitement.

L'exercice de ce droit n'est pas applicable aux traitements mis en œuvre à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales ou portant sur des soupçons d'activité illicite ainsi qu'aux traitements visés aux articles 74 et 87 du projet de loi.

L'article 17 introduit dans la législation monégasque un nouveau droit relatif à la portabilité des données. Il s'agit de permettre aux personnes concernées d'obtenir du responsable du traitement les données qu'elles lui ont fournies à un moment donné, à l'occasion de l'exécution d'un contrat par exemple.

Le droit à la portabilité renforce le contrôle que les personnes concernées exercent sur leurs propres données. Elles peuvent sauvegarder leurs données en vue d'un usage personnel ultérieur ou les transmettre à un autre responsable du traitement pour être réutilisées à d'autres fins. Ces données doivent leur être transmises dans un format couramment utilisé et lisible.

L'exercice de ce droit nécessite que trois conditions soient réunies : il doit être limité aux traitements fondés sur le consentement ou sur un contrat, ne s'appliquer que sur les données traitées de manière automatisée et ne pas porter atteinte aux droits et libertés des tiers.

Les données traitées sur la base d'obligations légales ou dans le cadre de l'exécution d'une mission d'intérêt général par une personne morale de droit privé ou concessionnaire d'un service public ou relevant de l'exercice de l'autorité publique ne sont pas considérées comme des données portables dès lors que, comme le précise le Règlement européen, « *de par sa nature même, ce droit ne devrait pas être exercé à l'encontre de responsables du traitement qui traitent des données à caractère personnel dans l'exercice de leurs missions publiques* ».

L'article 18 confère à la personne concernée, comme le permet déjà la loi n° 1.165 du 23 décembre 1993, modifiée, précitée le droit de ne pas être soumise à une décision produisant des effets juridiques à son égard ou l'affectant de manière significative, prise sur le seul fondement d'un traitement automatisé, y compris le profilage.

En l'état, le profilage et la prise de décision automatisée peuvent être des activités combinées relevant du même processus mais peuvent également être effectués séparément. Ainsi, dans certains cas, les décisions automatisées sont prises avec (ou sans) profilage et le profilage peut être ainsi réalisé sans prendre de décisions automatisées.

La technique du profilage consiste à évaluer les aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des aspects concernant le rendement au travail, sa situation économique, sa santé, ses préférences ou centres d'intérêt personnels, sa fiabilité ou son comportement, ou sa localisation et ses déplacements. Un tel traitement est interdit dès lors qu'il produit des effets juridiques à son égard ou qu'il l'affecte de manière significative. Ce droit protège la personne concernée face à des décisions impactant ses droits et libertés ou influençant son environnement, son comportement et son choix ou aboutissant à une discrimination.

À titre d'illustration, une décision est notamment considérée comme produisant des effets juridiques à l'égard d'une personne quand elle permet d'accorder ou de refuser un droit, par exemple au moyen d'un raisonnement algorithmique analysant le profil d'une personne au regard de critères permettant de bénéficier d'un avantage social particulier. De la même façon, l'évaluation de la capacité d'emprunt sur le seul fondement d'un logiciel est de nature à affecter significativement la situation d'une personne.

Des exceptions à cette interdiction sont toutefois admises, notamment lorsque la personne concernée a donné son consentement explicite ou si la décision automatisée est prévue par des dispositions législatives ou réglementaires.

En tout état de cause, lorsque l'une des exceptions s'applique, des mesures doivent être mises en place pour sauvegarder les droits et libertés de la personne concernée ainsi que ses intérêts légitimes. En effet, un traitement de cette nature doit être assorti de garanties appropriées qui peuvent consister en une information spécifique de la personne concernée ou le droit d'obtenir une intervention humaine, d'exprimer son point de vue, d'obtenir une explication quant à la décision prise à l'issue de ce type d'évaluation et de contester la décision.

L'article 19 concerne les personnes décédées. Bien que le R.G.P.D. et la Convention 108+ ne soient pas applicables aux personnes décédées, ils laissent néanmoins la possibilité aux États de prévoir des règles relatives au traitement des données à caractère personnel desdites personnes. Tel est l'objet de cet article qui permet, sauf dispositions législatives contraires, à l'ascendant, au descendant jusqu'au second degré, au conjoint survivant d'une personne décédée, s'il justifie d'un intérêt, d'exercer les droits prévus aux articles 11, 12, 13, 14, 16 et 17 pour ce qui est des informations la concernant. Le Gouvernement a également entendu faire référence à la loi n° 1.481 du 17 décembre 2019 sur le contrat civil de solidarité, en visant expressément le cohabitant ou le partenaire au sens de ladite loi.

L'article 20 du projet de loi concerne les limitations pouvant être apportées à certains droits et obligations dès lors que le droit à la protection des données n'est pas un droit absolu et qu'il peut être limité pour servir un objectif d'intérêt général, un but légitime ou encore pour répondre au besoin de protection des droits et libertés d'autrui.

Il se rattache à l'article 23 du Règlement européen et à l'article 11 de la Convention 108 modernisée, et permet au responsable du traitement ou au sous-traitant, dans son premier alinéa, de faire exception à l'exercice des droits des personnes concernées pour des finalités bien déterminées au regard de ces buts légitimes ou des « *objectifs essentiels d'intérêt public général* », pour reprendre l'expression de la Convention 108 modernisée. Il s'agit notamment de garantir la sécurité nationale ou la sécurité publique, la prévention des infractions pénales, l'indépendance de la justice et des procédures judiciaires ou encore les intérêts économiques et financiers, dans les domaines monétaire, budgétaire et fiscal, la santé publique ou la sécurité sociale ou encore la liberté d'expression publique.

Les droits concernés par la limitation sont ceux visés aux articles 9 à 18 du projet de loi. Peuvent également être limitées les caractéristiques des données visées à l'article 4 ainsi que la notification d'une violation de données à caractère personnel à la personne concernée.

Pour qu'il puisse être fait exception à ces dispositions, une double condition est requise : d'une part, le responsable du traitement ou le sous-traitant doit intervenir dans le cadre des missions qui lui sont légalement conférées et, d'autre part, l'exception doit respecter les droits et libertés fondamentaux et constituer une mesure nécessaire et proportionnée.

Il est précisé que le terme « *légalement* » signifie que la chose est réalisée de manière conforme aux règles juridiques en vigueur, de quelque nature qu'elles soient et non pas seulement conforme à la loi, au sens propre que revêt cette norme juridique.

Si le premier alinéa de l'article 20 énonce les domaines dans lesquels peuvent s'appliquer des exceptions à l'exercice des droits, le second alinéa sécurise les conditions juridiques dans lesquelles s'exercent ces exceptions en prévoyant qu'elles soient visées dans l'acte juridique qui crée le traitement.

Le Chapitre IV porte sur les obligations incombant au responsable du traitement et au sous-traitant. Il comporte deux sections qui distinguent les obligations générales de celles plus spécifiques tenant à la nature des traitements.

L'article 21 introduit la notion de « *responsabilisation* » du responsable du traitement, lequel doit s'assurer que le traitement mis en œuvre est effectué dans le respect des dispositions de la loi et être en mesure de le démontrer. Il pose également l'obligation pour le responsable du traitement, le sous-traitant et leurs représentants, de coopérer avec l'autorité de protection, à la demande de celle-ci, dans l'exécution de ses missions.

L'article 22 pose le principe de protection des données dès la conception du traitement, c'est à dire dès sa phase de création et tout au long de son cycle de vie. L'application de ce principe implique que le responsable du traitement évalue l'impact potentiel de son traitement sur les droits et libertés des personnes concernées et ce, de façon régulière afin qu'il mette en œuvre des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation ou la minimisation des données, pour s'assurer que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement soient traitées.

Les finalités du traitement doivent être définies avec précision dès la conception du projet afin que s'appliquent les principes de limitation des finalités et de minimisation de la collecte.

L'article 23 prévoit la possibilité que les moyens et les finalités du traitement soient déterminés par plusieurs responsables du traitement. Il pourra s'agir par exemple de la création et de l'utilisation d'une plateforme commune sur internet par deux responsables du traitement proposant des services différents. Ils seront responsables conjoints du traitement lié à la création du site internet. Dans ce cas, un accord de responsabilité conjointe doit être défini entre eux afin que les obligations leur incombant au titre de la présente loi soient respectées et que l'exercice des droits des personnes concernées soit assuré.

L'article 24 du projet de loi prévoit la désignation d'un représentant sur le territoire monégasque, comme le fait déjà l'article 24 de la loi n° 1.165 du 23 décembre 1993, modifiée, précitée.

En raison du caractère extraterritorial du champ d'application du projet de loi, cette obligation n'est plus uniquement liée au recours à des moyens de traitement situés à Monaco mais au fait que les responsables du traitement ou les sous-traitants, non établis à Monaco, proposent des produits ou des services à des personnes situées sur le territoire de la Principauté ou mettent en œuvre des traitements relatifs au suivi de leur comportement.

Par exemple, une entreprise d'e-commerce établie dans un État membre de l'Union européenne et proposant des produits ou des services à des personnes situées sur le territoire de la Principauté devra y désigner un représentant. Il en ira de même pour une entreprise de presse américaine qui propose un service d'abonnement en ligne à un journal sans disposer de bureau à Monaco.

Cette obligation n'est pas générale mais comporte des exceptions lorsque le traitement est occasionnel, s'il est relatif à des condamnations pénales ou à des infractions ou si le responsable du traitement est un organisme du secteur public. À Monaco, les organismes du secteur public sont définis comme des « *personnes morales de droit public, autorités publiques, organismes de droit privé investis d'une mission d'intérêt général ou concessionnaires d'un service public* » définition qui correspond globalement à celle du règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur.

L'article 25 encadre le recours à la sous-traitance et prévoit les clauses minimales que doit contenir le contrat. Il impose au responsable du traitement, de ne recourir qu'à des sous-traitants présentant des garanties suffisantes au regard des principes de protection des données prévus par le présent projet de loi. Le sous-traitant pourra faire valoir l'application d'un code de conduite ou un mécanisme de certification pour démontrer l'existence de garanties suffisantes pour respecter les droits des personnes concernées.

L'article 26 introduit l'obligation de tenue d'un registre des activités du traitement pour les responsables du traitement et les sous-traitants. La tenue de ce registre se substitue, en quelque sorte, aux formalités préalables prévues par la loi n° 1.165 du 23 décembre 1993, modifiée, précitée et a pour objectif d'identifier clairement les traitements mis en œuvre et d'en faciliter le suivi.

Il s'agit d'un outil de conformité introduit par le R.G.P.D. qui permet de démontrer à l'autorité de protection, lorsqu'elle en fait la demande, la licéité du traitement et sa conformité aux règles prévues par la présente loi. C'est également un outil de pilotage pour le responsable du traitement et le sous-traitant car il leur permet de recenser l'ensemble des opérations de traitement et les catégories de données personnelles collectées.

L'obligation de tenue du registre n'est pas de portée générale. Le R.G.P.D. fixe à 250 employés le seuil à partir duquel la tenue du registre est obligatoire mais prévoit une dérogation pour tenir compte de la situation particulière des micros, petites et moyennes entreprises. Tenant compte des besoins spécifiques des micros, petites et moyennes entreprises dans le contexte de la Principauté, le seuil de cinquante salariés a été retenu pour rendre obligatoire la tenue de ce registre aux acteurs économiques monégasques. Ce seuil est déjà connu à Monaco puisque c'est celui à partir duquel une entreprise à l'obligation d'instituer un comité d'hygiène et de sécurité. Ainsi, tout en prenant en compte le tissu économique de la Principauté le seuil de 50 salariés assure un niveau élevé de protection des données puisqu'il soumet à cette obligation plus de 2% des structures installées en Principauté alors que ce taux est inférieur à 1% dans les autres pays, notamment de l'Union européenne.

Toutefois, si le traitement est susceptible de comporter un risque pour les droits et libertés des personnes concernées ou s'il n'est pas occasionnel, ou s'il porte sur des données sensibles ou sur des données personnelles relatives à des infractions, des condamnations pénales et mesures de sûreté ou portant sur des soupçons d'activités illicites, le seuil ne s'applique pas et le responsable du traitement devra tenir un registre, quel que soit le nombre de ses salariés.

L'article 27 introduit la fonction de « *délégué à la protection des données* ». Selon le Comité européen, le délégué à la protection des données est l'une des « *pierres angulaires du régime de responsabilité* » en facilitant le respect des règles et en favorisant la conformité du traitement à la réglementation. C'est un acteur clé dans le nouveau système de gouvernance des données.

Le délégué agit comme intermédiaire entre les acteurs concernés, à savoir l'autorité de protection, les personnes concernées et les entités économiques ou les autorités administratives qui l'ont désigné.

Cette désignation est obligatoire pour les personnes morales de droit public et organismes de droit privé investis d'une mission d'intérêt général ou concessionnaires d'un service public.

Les missions du délégué sont précisément définies. Il a un rôle d'accompagnement, de conseil, d'information, de contrôle et de coopération avec l'autorité de protection. Il doit disposer d'une autonomie et de ressources suffisantes pour s'acquitter efficacement de ses missions.

Le délégué à la protection des données ne peut être relevé de ses fonctions ou pénalisé par le responsable du traitement ou le sous-traitant pour l'exercice de ses missions et n'est pas personnellement responsable en cas de non-respect de la loi. C'est le responsable du traitement qui est tenu de s'assurer et d'être en mesure de démontrer que le traitement est effectué conformément à la loi en vertu des dispositions de l'article 21 et le cas échéant le sous-traitant, si en violation de la loi il détermine les finalités et les moyens du traitement comme le prévoit l'avant-dernier alinéa de l'article 25.

Un même délégué peut être désigné pour un groupe d'entreprises à la condition qu'il soit facilement joignable à partir de chaque lieu d'établissement, comme par exemple une succursale d'un établissement bancaire.

Le projet de loi prévoit également que le délégué désigné par l'État aura une mission spécifique auprès de l'autorité de protection consistant à présenter le dossier de demande d'avis lorsque le traitement concerné est lié à la souveraineté de l'État, à savoir lorsqu'il porte sur l'une des finalités prévues aux articles 61 et 74.

Pour l'exercice de sa mission, le délégué peut accéder aux données et aux opérations de traitement, à l'exception toutefois des traitements visés aux articles 61 et 87 eu égard à la confidentialité des informations qu'ils contiennent.

L'article 28 précise les obligations de sécurité mises à la charge du responsable du traitement et du sous-traitant.

Ainsi, conformément au principe de responsabilisation, l'adoption de mesures de sécurité appropriées nécessite une analyse permettant d'identifier les risques puis de déterminer leur niveau de probabilité et de gravité.

Les risques pris en considération sont soit d'ordre technique – notamment la destruction, la perte ou l'indisponibilité des données – soit relatifs aux droits et libertés des personnes, par exemple lorsque la réalisation du traitement est susceptible de conduire à une discrimination, une usurpation d'identité ou au dévoilement d'informations couvertes par le secret professionnel.

A titre d'exemple, les mesures de sécurité pourraient plus spécifiquement porter sur le contrôle de l'accès aux installations, des supports de données et de la conservation des données, des utilisateurs, de l'accès aux données aux seules personnes autorisées, de la transmission aux destinataires, de l'introduction des données, du transport des supports de données, de la restauration en cas d'interruption du système de traitement, du contrôle de la fiabilité et de l'intégrité du système de traitement lorsque le traitement est mis en œuvre dans le cadre des articles 61, 74 et 87 du projet de loi. Dès lors que ces traitements sont soumis à l'avis de l'autorité de protection ou de la Commission de l'article 16, ces autorités seront en capacité d'apprécier les mécanismes de sécurité proposés ou mis en place et de faire toute proposition le cas échéant.

Il est par ailleurs prévu que l'application d'un code de conduite ou d'un mécanisme de certification tels que visés aux articles 30 et 31 du projet de loi peut servir d'élément au responsable du traitement ou au sous-traitant pour démontrer le respect des exigences en matière de sécurité.

L'article 29 détermine les obligations des responsables du traitement en matière de notification à l'autorité de protection d'une violation de données à caractère personnel dont il a connaissance et de communication de cette violation à la personne concernée. La notification à l'autorité de protection a pour objectif d'assurer une intervention permettant de préserver les droits et libertés des personnes concernées par la violation.

Si la violation est susceptible d'engendrer un risque élevé pour la personne concernée, le responsable du traitement est tenu d'informer la personne concernée dans les meilleurs délais. Cette appréciation du risque se fait à la lumière d'un incident particulier et repose sur les conséquences qui en découlent. Ainsi, elle tient compte, notamment, du type de violation, du caractère sensible ou du volume des données, de la facilité d'identification des personnes concernées, de la gravité des conséquences pour les personnes concernées et de la probabilité qu'elle se reproduise.

Des dérogations sont prévues à l'obligation de communication de la violation à la personne concernée, notamment si cette communication nécessite des efforts disproportionnés pour le responsable du traitement ou si les données ont fait l'objet de chiffrement par exemple qui les rendent incompréhensibles.

L'article 30 est relatif à l'établissement de codes de conduite par des associations et des organismes professionnels représentant des catégories de responsables du traitement ou de sous-traitants. Les codes de conduite font partie des nouveaux outils de conformité mis en place par le R.G.P.D. qui permettent de répondre, dans un secteur particulier, aux besoins opérationnels des professionnels dans leur démarche de conformité en matière de protection des données.

Bien que s'agissant d'une initiative volontaire pour encourager les professionnels à adopter des bonnes pratiques et usages et de démontrer, auprès des personnes concernées et autres acteurs, le respect des dispositions applicables aux traitements de données à caractère personnel, les codes de conduites revêtent un caractère obligatoire pour leurs adhérents.

L'autorité de protection pourra être appelée à adopter des recommandations ou des lignes directrices pour accompagner les porteurs de projet de code de conduite. Lorsque le code de conduite a déjà été approuvé par une autorité de protection étrangère, l'autorité vérifie que ses dispositions contiennent les garanties de protection appropriées au regard de la loi monégasque préalablement à sa validation.

L'article 31 instaure une procédure de certification en matière de protection des données pouvant être mise en œuvre directement par l'autorité de protection ou par des organismes indépendants agréés par cette dernière. La mise en place de mécanismes de certification en matière de protection des données permet de démontrer que les opérations de traitement effectuées par les responsables du traitement et les sous-traitants respectent la présente loi. La certification est un processus volontaire qui ne diminue pas la responsabilité du responsable du traitement ou du sous-traitant.

L'organisme demandant l'agrément doit justifier d'une expertise au regard de l'objet de la certification et répondre à des critères pris par arrêté ministériel sur proposition de l'autorité de protection.

Le projet de loi prévoit également la faculté de reconnaissance, par l'autorité de protection monégasque, des certifications délivrées par un organisme agréé d'un pays membre de l'Union européenne ou justifiant d'un niveau de protection adéquat, cette démarche étant de nature à faciliter l'accès au marché monégasque pour les acteurs certifiés à l'étranger.

L'article 32 instaure l'obligation de réaliser une analyse d'impact relative à la protection des données par le responsable du traitement pour les opérations de traitements les plus sensibles entraînant un risque élevé pour les droits et libertés des personnes concernées.

Il s'agit d'un processus dont l'objet est de décrire le traitement, d'en évaluer la nécessité et la proportionnalité, d'évaluer les risques pour les droits et libertés des personnes physiques liés au traitement de leurs données à caractère personnel et de déterminer les mesures nécessaires pour y faire face.

Quatre situations de risque élevé sont notamment visées dans le projet de loi :

- lorsque le traitement permet une évaluation systématique ou un profilage. Il en est ainsi en cas d'évaluation ou de notation de la personne sur son rendement au travail, sa santé, sa situation économique, son comportement, ses centres d'intérêt ou sa localisation ;

- lorsque le traitement porte sur des données sensibles ou relatives à des infractions, condamnations pénales ou portant sur des soupçons d'activité illicite, et qu'il est réalisé à grande échelle. Il peut s'agir, par exemple, de traitements de données de santé réalisés par un établissement hospitalier ou de traitements portant sur des déclarations de soupçon réalisés par un établissement bancaire ;

- une analyse d'impact devra également être effectuée en cas de surveillance systématique réalisée à grande échelle d'une zone accessible au public, comme par exemple un centre commercial ou une galerie marchande ;

- lorsque le traitement fait usage, à grande échelle, d'un identifiant numérique.

Au-delà de ces situations, une analyse d'impact pourra s'avérer nécessaire dans d'autres circonstances de risque élevé. Dans le cadre de ses missions, l'autorité de protection sera amenée à adopter des recommandations ou des lignes directrices identifiant, à partir d'une liste de critères adoptée par arrêté ministériel, les traitements les plus susceptibles de nécessiter une analyse d'impact.

Pour apprécier si un traitement est effectué à grande échelle, différents éléments peuvent être pris en considération : il peut s'agir du volume de données à caractère personnel traité, du nombre de personnes concernées que ce soit en valeur absolue ou en fonction de la population considérée, de l'étendue géographique du traitement, de la durée ou de la permanence de l'activité de traitement.

Le R.G.P.D. considère que le traitement n'est pas réalisé à grande échelle lorsqu'il est effectué par un médecin ou un avocat exerçant à titre individuel qui traite les données de ses patients ou de ses clients. Dans ces cas, une analyse d'impact n'est pas nécessaire, même en présence de données sensibles.

L'analyse d'impact n'est pas requise pour les traitements qui demeurent soumis à l'avis préalable de l'autorité de protection ou de la Commission de l'article 16 de la loi n° 1.430 du 13 juillet 2016, précitée, dans la mesure où il revient à ces autorités d'apprécier le niveau de risque dans le cadre de l'avis.

L'article 33 organise un contrôle *a priori* en prévoyant la consultation de l'autorité de protection lorsque l'analyse d'impact fait apparaître un risque élevé non maîtrisé par le responsable du traitement. En effet, si au terme de l'analyse prévue à l'article 32, le responsable du traitement considère que les risques identifiés ne peuvent pas être suffisamment réduits et qu'il existe des risques résiduels élevés, il est tenu de consulter l'autorité de protection. Celle-ci dispose d'un délai maximum de huit semaines pour rendre un avis écrit au responsable du traitement, délai qui peut être prolongé de six semaines lorsqu'il s'agit d'un traitement complexe. L'autorité de protection peut imposer des mesures appropriées si elle considère que le traitement constituerait en l'état une violation.

Le Chapitre V est consacré à l'Autorité de Protection des Données Personnelles. Il comporte deux sections relatives au fonctionnement de l'autorité et au contrôle de la mise en œuvre des traitements.

La section I concerne le fonctionnement de l'autorité de protection.

L'article 34 crée une nouvelle autorité administrative indépendante qui succède à la Commission de Contrôle des Informations Nominatives (C.C.I.N.).

Dénommée Autorité de Protection des Données Personnelles (A.P.D.P.), cette autorité est chargée de contrôler et vérifier que les données personnelles sont traitées en conformité avec les dispositions législatives et réglementaires en vigueur relatives à la protection des données à caractère personnel.

Cet article prévoit la mise en place d'une formation restreinte de l'autorité de protection dont la composition est définie à l'article 38.

La création de la formation restreinte se différencie de l'architecture retenue par la loi n°1.165 du 23 décembre 1993, précitée, qui accorde au Président de la C.C.I.N. le pouvoir de décider des contrôles, de l'opportunité des poursuites et de prononcer des sanctions administratives.

En instaurant une formation restreinte dotée du pouvoir de prendre les mesures et de prononcer les sanctions à l'encontre des responsables du traitement ou des sous-traitants, le projet de loi permet d'assurer une plus grande conformité aux exigences européennes en distinguant le mécanisme de poursuite et de sanction, conformément aux dispositions de l'article 6 de la Convention Européenne des Droits de l'Homme. Ainsi, la formation plénière serait chargée de déterminer l'opportunité des poursuites et la formation restreinte serait chargée de prononcer les sanctions.

En revanche, comme le permettent la Convention 108+ et le droit de l'Union, le chiffre 1 de l'article 34 exclut des compétences de l'autorité de protection les traitements effectués par les juridictions et le ministère public dans l'exercice de leurs fonctions juridictionnelles ainsi que ceux effectués dans le cadre des procédures d'entraide judiciaire internationale afin de préserver l'indépendance du pouvoir judiciaire. Pour autant, il est prévu que les traitements de ces autorités demeurent soumis à un contrôle spécifique au sein de l'appareil judiciaire, par la désignation d'un Délégué judiciaire à la protection des données.

Le chiffre 2 prévoit par ailleurs, comme exposé ci-avant, de confier le contrôle des traitements qui intéressent la sûreté de l'État et la sécurité nationale régis par les dispositions des articles 9 à 15 et 18 de la loi n°1.430 du 13 juillet 2016 portant diverses mesures relatives à la préservation de la sécurité nationale à la Commission instituée par l'article 16 de ladite loi, qui revêt le caractère d'autorité de contrôle indépendante.

Les articles 9 à 15 de ladite loi sont relatifs aux interceptions de correspondances pour la prévention du terrorisme et pour la sauvegarde des intérêts fondamentaux de la Principauté et aux techniques spéciales d'investigation pour les mêmes finalités. Il s'agit de traitements spécifiques d'activités de renseignements dont le régime juridique relève de la loi sur la sécurité nationale et des dispositions prévues par la section VI du chapitre VII de la présente loi.

Le renvoi à l'article 18 de la loi n° 1.430 du 13 juillet 2016, précitée, relatif au secret de sécurité nationale, lequel comporte plusieurs niveaux de classification, s'explique dès lors que le traitement comporte des informations classifiées au sens de cet article et qu'il est donc couvert par le secret de sécurité nationale et que la cohérence d'action implique son contrôle par la Commission instituée par l'article 16 de ladite loi, appelée également à se prononcer sur la déclassification des informations.

L'article 35 définit précisément les missions de la nouvelle autorité de protection qui ont été renforcées. Elles s'inscrivent dans la perspective de la reconnaissance du caractère adéquat de la législation monégasque par la Commission européenne et de la ratification de la Convention 108 modernisée du Conseil de l'Europe.

Au titre de ces missions, figure en premier lieu celle de favoriser l'information du public sur ses fonctions, ses pouvoirs et ses activités ainsi que sa compréhension des risques, des règles, des garanties et des droits relatifs à la protection des données personnelles en portant une attention particulière au droit à la protection des données des enfants et des personnes dites « vulnérables » entendues notamment, comme, en sus des enfants, les salariés, les personnes handicapées, les personnes âgées…

L'autorité a également une mission de conseil, d'accompagnement des responsables du traitement, des sous-traitants et des personnes concernées, lesquelles sont de plus en plus attentives au traitement de leurs données.

Elle dispose du pouvoir d'intervention en faisant procéder d'office ou sur signalement à des vérifications et à des investigations en cas de manquements aux dispositions de la présente loi et doit tenir des registres internes des violations de la loi et des mesures correctrices prises par ses soins.

L'autorité continuera à formuler des avis sur les traitements qui lui seront soumis par les autorités administratives et judiciaires compétentes dans le cadre prévu par la loi ainsi qu'au titre des analyses d'impact lorsque son avis devra être requis.

Le projet de loi confère de nouvelles attributions à l'autorité de protection au titre desquelles peut être citée l'adoption de recommandations mais également de lignes directrices destinées à faciliter l'application des règles prévues par la présente loi, notamment en matière de certification, de code de déontologie et d'analyse d'impact.

L'autorité est consultée pour avis par le Ministre d'État sur l'élaboration de mesures législatives ou réglementaires mais également par le Secrétaire d'Etat à la Justice, Directeur des Services Judiciaires sur des projets d'arrêtés directoriaux dans le cadre de l'administration de la justice relatifs à la protection des données à caractère personnel ou au traitement de telles données mais peut l'être également sur toutes mesures ayant trait à la protection des données. Elle peut être également consultée par le Président du Conseil National sur des propositions de loi concernant la protection des données ou le traitement de telles données.

Les avis de l'autorité sont rendus publics par l'autorité consultante mais également par l'autorité de protection avec l'accord de cette dernière. Il s'agit là d'une avancée importante du projet de loi en matière de saisine et de transparence des avis de l'autorité de protection.

L'autorité dispose également d'un pouvoir d'initiative en ayant la faculté de proposer au Ministre d'État l'adoption de mesures particulières de protection des données à l'égard de l'utilisation des nouvelles technologies, ce qui vient reconnaître sa compétence spécifique en ce domaine.

L'article 36 est consacré à la saisine de l'autorité de protection qui s'exerce sans préjudice de tout autre recours juridictionnel dès lors qu'il ne constitue pas une voie de recours exclusive ni obligatoire.

L'autorité de protection doit informer la personne concernée de l'état d'avancement de sa réclamation et de l'existence de ce recours juridictionnel effectif.

Les réclamations concernant les traitements mis en œuvre par les juridictions dans l'exercice de leurs fonctions juridictionnelles et par le ministère public relèvent, quant à elles, de la juridiction compétente pour statuer sur le litige ou la procédure au cours desquels les données ont été collectées.

L'article 37 définit les modalités de nomination et de composition de l'autorité de protection dont le nombre est porté de 6 à 8 membres. Cette majoration répond à la nécessité de disposer de compétences spécifiques dans le secteur de la santé et dans le domaine juridictionnel. L'importance du secteur de la santé au regard de la protection des données justifie la désignation d'un membre ayant des connaissances spécifiques, proposé par le Comité de la Santé Publique.

Dans le domaine juridictionnel, la création d'une formation restreinte conduit à la nécessité de prévoir deux magistrats. Un magistrat désigné par le premier Président de la Cour de Révision pour conduire les investigations dans le domaine judiciaire et pour les traitements visés à l'article 61, et un magistrat désigné par le premier Président de la Cour d'Appel, destiné à présider la formation restreinte. Dans le souci de respecter la séparation des pouvoirs de poursuite et des pouvoirs de sanction, le magistrat chargé des investigations ne siège pas dans la formation restreinte.

La désignation de magistrats suppléants permet de garantir la continuité des missions de l'autorité de protection en cas d'empêchement d'un magistrat, au sens judiciaire du terme.

Comme pour la désignation des membres de la C.C.I.N., il est prévu, afin de garantir leur indépendance, que les membres de l'autorité sont désignés hors de l'institution qui les propose, à l'exception des magistrats qui peuvent être en activité.

Le président et le vice-président de l'autorité sont élus en son sein à la majorité absolue. Ils ne peuvent siéger dans la formation restreinte.

Enfin, le projet de loi introduit une disposition qui permet d'assurer la continuité dans le fonctionnement de l'autorité lorsqu'un membre cesse ou n'est plus en mesure d'exercer son mandat, dont la durée est de 5 ans renouvelable une fois.

L'article 38 précise la composition de la formation restreinte qui comprend trois membres. Présidée par le magistrat du siège, les deux autres membres sont élus par l'autorité de protection. La formation restreinte est chargée de prononcer les sanctions prévues à l'article 48 à l'encontre des responsables du traitement ou des sous-traitants qui ne respectent pas les dispositions de la présente loi. A ce titre, ses membres ne peuvent exercer aucune attribution en matière d'instruction et de poursuites.

L'article 39 prévoit les incompatibilités applicables aux membres de l'autorité afin de garantir leur indépendance. Prévues aujourd'hui dans l'ordonnance souveraine n°2.230 du 19 juin 2009 fixant les modalités d'application de la loi n° 1.165 du 23 décembre 1993, modifiée, précitée, ces incompatibilités figurent désormais dans le corps de la loi.

Le projet de loi renforce l'incompatibilité relative à l'exercice de fonctions ou la détention de participations dans des entreprises monégasques ou étrangères concourant à la fabrication de matériel utilisé en informatique ou en communications électroniques ou à la fourniture de services en informatique ou en communications électroniques, par l'ajout d'entreprises concourant au commerce de biens matériels et immatériels ou de prestations de service dans ces domaines.

L'article 40 est relatif à la confidentialité. Les membres de l'autorité de protection, le personnel de ses services ainsi que toute personne dont elle s'assure le concours, sont tenus au secret professionnel et à une obligation de discrétion y compris après la fin de leur mandat ou de leurs fonctions par rapport aux éléments qu'ils ont eu à connaître en raison de leur mandat ou de leurs fonctions. En cas de manquement à ces obligations, des peines différentes sont applicables selon la nature du manquement.

L'article 41 concerne l'organisation de l'autorité de protection. Il détermine son fonctionnement budgétaire et organisationnel, les pouvoirs de représentation du président et les règles applicables aux personnels de ses services, ce qui confère à l'autorité les attributs indispensables de fonctionnement pour être une autorité administrative indépendante au sens des critères européens de protection des données.

Le président de l'autorité de protection est chargé de représenter l'État en justice à raison des activités et du fonctionnement de ladite autorité, laquelle est tenue par ailleurs d'établir et de publier son règlement intérieur.

L'article 42 pose le principe d'une coopération de l'autorité de protection avec ses homologues étrangères chargées de la protection des données qui offrent un niveau de protection équivalent ou approprié. La coopération entre autorités de protection permet notamment d'échanger des informations pertinentes, de coordonner les investigations et de conduire des actions conjointes.

La coopération peut cependant être refusée dans certaines situations précisément définies comme par exemple lorsque la demande n'entre pas dans la compétence de l'autorité ou si la réciprocité n'est pas garantie.

La section II prévoit les dispositions applicables en matière de contrôle de la mise en œuvre des traitements.

L'article 43 confère à l'autorité de protection les pouvoirs d'investigation. Ces pouvoirs correspondent à ceux qu'exerce déjà la C.C.I.N. au titre de la loi n° 1.165 du 23 décembre 1993, précitée, modifiée à cet égard par la loi n° 1.420 du 1er décembre 2015 portant modification des articles 18 et 19 de la loi n° 1.165 du 23 décembre 1993 relative à la protection des informations nominatives, modifiée.

La nouvelle répartition entre les pouvoirs d'investigation dévolus à l'autorité et les pouvoirs de sanction exercés par la formation restreinte, assure opportunément un partage de compétence au sein de l'autorité de protection

Cet article précise et encadre les pouvoirs dévolus aux agents et investigateurs lors de leurs opérations de contrôle. Il est prévu que lorsque les investigations ou vérifications portent sur un traitement mis en œuvre par le Secrétaire d'Etat à la Justice, Directeur des Services Judiciaires, par les juridictions et par le ministère public hors de leurs fonctions juridictionnelles, le président de l'autorité de protection désigne le magistrat visé au chiffre 7 de l'article 37 pour procéder auxdites investigations ou vérifications, ou son suppléant en cas d'empêchement.

La réalisation des investigations de cette nature par un magistrat tient à préserver l'indépendance de la justice et la séparation des pouvoirs. Ledit magistrat procède également aux vérifications ou investigations lorsqu'elles concernent l'un des traitements visés à l'article 61.

Le projet de loi prévoit, par ailleurs, que les investigations ou vérifications portant sur un traitement mis en œuvre par les juridictions et par le ministère public dans l'exercice de leurs fonctions juridictionnelles s'opèrent par le Délégué judiciaire à la protection des données désigné par le Secrétaire d'État à la Justice, Directeur des Services Judiciaires.

L'article 43 introduit également la possibilité pour les agents et les investigateurs de faire usage d'une identité d'emprunt à l'occasion d'un contrôle en ligne comme cela se pratique déjà en France.

L'article 44 pose le principe, dans son premier alinéa, que le secret ou une obligation de confidentialité ne peuvent être opposé dans le cadre des investigations menées par l'autorité de protection.

Il prévoit cependant des exceptions applicables au secret de sécurité nationale, au secret professionnel concernant les relations entre un avocat et son client, au secret des sources journalistiques et au secret médical.

Le secret de sécurité nationale est opposable, quel que soit le niveau de classification, dès lors qu'il est destiné à sauvegarder les intérêts fondamentaux de la Principauté, au sens des dispositions de l'article 18 de la loi n° 1.430 du 13 juillet 2016, précitée. Toutefois, le secret de sécurité nationale ne doit pas empêcher l'autorité de protection d'assurer ses missions de contrôle des traitements relevant de sa compétence qui seraient hébergés dans une zone protégée par ledit secret.

Le secret médical est également opposable en matière de données de santé et seul un médecin est habilité à en connaître.

L'article 45 permet au responsable du traitement ou au sous-traitant de s'opposer aux investigations de l'autorité de protection. Lorsque ce droit est exercé, les opérations de contrôle ne peuvent avoir lieu qu'après l'autorisation du Président du Tribunal de première instance, saisi sur requête par le président de l'autorité de protection.

En cas de risque imminent de destruction ou de disparition de pièces ou de documents nécessaires aux investigations, le responsable du traitement ne peut s'opposer aux opérations de vérifications et d'investigation lesquelles peuvent faire l'objet dans tous les cas d'un recours devant le Tribunal de première instance.

L'article 46 confère à l'autorité le pouvoir d'accéder aux locaux et établissements du responsable du traitement lorsqu'il existe des raisons de soupçonner que la mise en œuvre des traitements n'est pas conforme aux dispositions de la loi. L'exercice de ce pouvoir est cependant assorti d'une autorisation judiciaire préalable compte tenu des retombées et des conséquences d'un tel pouvoir sur les libertés et les droits des personnes contrôlées.

Cet article définit ainsi les conditions dans lesquelles les agents et investigateurs peuvent accéder aux locaux avec l'autorisation préalable du Président du Tribunal de première instance.

L'article 47 est particulièrement novateur en ce qu'il instaure des mesures préalables aux sanctions administratives. Il confère au président de l'autorité des pouvoirs correctifs lui permettant de signaler la méconnaissance des dispositions de la loi à un responsable du traitement ou à un sous-traitant et de le mettre en demeure de prendre les mesures nécessaires pour se mettre en conformité avec les dispositions de la loi lorsque le manquement est susceptible de faire l'objet d'une mise en conformité. Ces mesures, dites correctrices, qui ne constituent en aucune manière une sanction, relèvent du pouvoir du président de l'autorité et sont généralement préalables à une procédure de sanction.

Lorsque le traitement a été mis en conformité, le président de l'autorité de protection prononce la clôture de la procédure de mise en demeure qui peut être rendue publique.

En cas de non mise en conformité ou lorsque le manquement ne peut faire l'objet d'une mise en conformité car il ne peut donner lieu à une mesure corrective, comme par exemple, un transfert litigieux a été opéré ou que des données ont été détruites, ou lorsque le responsable du traitement ou le sous-traitant ne respecte pas les obligations de la loi, l'article 48 prévoit que le président de l'autorité de protection peut, sans avoir à lui adresser la mise en demeure, saisir la formation restreinte en vue du prononcé d'une sanction sur la base d'un rapport établi par l'un des membres de l'autorité de protection désigné par le président, hors formation restreinte. À l'issue d'une procédure contradictoire, la sanction est prononcée à l'encontre de l'entité juridique, personne physique ou morale mise en cause qui assume la responsabilité des traitements ou qui a été qualifiée de sous-traitant**.** La formation restreinte peut décider de prendre une ou plusieurs mesures parmi les sanctions prévues et cumuler une amende administrative à une limitation temporaire du traitement, par exemple.

Le projet de loi maintient la faculté, introduite en 2015, de pouvoir procéder, pour la formation restreinte, à la publicité des décisions qu'elle prend. Cette publicité est susceptible de recours devant le Tribunal de première instance si elle est de nature à créer un préjudice grave et disproportionné à la sécurité publique, au respect de la vie privée et familiale ou aux intérêts légitimes du responsable du traitement.

S'agissant des traitements de l'État et de la Commune, les sanctions peuvent consister en un avertissement ou une obligation de mise en conformité du traitement, non assortie d'astreinte. La possibilité de prononcer des sanctions financières contre l'Etat et la Commune n'a pas été retenue selon le principe d'effectivité des sanctions prévu par la Convention 108 modernisée. En effet, de telles sanctions seraient sans effet « *comminatoire* » ou dissuasif puisque les amendes seraient prélevées sur le Budget de l'État pour ensuite être reversées à ce même budget, l'autorité de protection n'étant pas dotée d'un patrimoine propre.

Le projet de loi prévoit la possibilité d'assortir l'obligation de mise en conformité d'une astreinte dont le montant fixé à 1 000 € (mille euros) par jour de retard peut être considéré comme suffisamment dissuasif.

Enfin, il précise que les manquements constitutifs d'infractions pénales sont signalés sans délai au Procureur Général.

L'article 49 détermine les éléments à prendre en compte par la formation restreinte pour que l'amende soit effective, proportionnée et dissuasive.

Ces critères, tels que la nature du manquement, sa gravité et sa durée ou encore le caractère délibéré de négligence ou de répétition du manquement, permettent d'individualiser la sanction en prenant en compte les circonstances propres à l'acteur poursuivi et au traitement litigieux.

Les modalités de notification de l'amende seront déterminées par voie réglementaire.

Les articles 50 et 51 fixent le montant maximum des amendes pouvant être appliquées par la formation restreinte en fonction des différents types de violation. Deux niveaux d'amende sont prévus par référence à la classification du R.G.P.D.

L'article 50 détermine le premier niveau d'amende en visant les types d'infractions pour lesquelles une amende peut être appliquée avec un plafond de 500 000 euros.

L'article 51 prévoit un plafond de 900 000 euros pour des catégories de manquements plus graves. Si ces montants peuvent apparaitre modestes au regard de ceux fixés par le R.G.P.D, à savoir dix millions d'euros pour le premier niveau et vingt millions d'euros pour le second, les montants proposés revêtent néanmoins un caractère dissuasif et répressif adapté au tissu économique local.

L'article 52 fixe les conditions de recouvrement de l'amende qui est versée à la Trésorerie Générale des Finances.

L'article 53 établit une procédure d'urgence permettant au président de l'autorité de protection de saisir la formation restreinte afin que celle-ci puisse prendre des mesures provisoires à titre conservatoire, pour une période ne pouvant excéder 6 mois, lorsque les libertés et droits fondamentaux des personnes physiques consacrés par le titre III de la Constitution sont violés. En cas d'atteinte grave et immédiate à ces droits, le président de l'autorité peut également saisir le Président du Tribunal de première instance par la voie du référé.

L'article 54 offre la garantie d'un recours effectif devant le Tribunal de première instance à l'encontre des décisions de la formation restreinte.

Le Chapitre VI est relatif aux traitements soumis à formalités préalables.

Bien que la nouvelle logique de responsabilisation prévue par la présente loi conduise à ce que la plupart des formalités préalables soient supprimées, le Gouvernement a fait le choix de maintenir des formalités pour certaines catégories de traitements visées au Chapitre VI.

L'article 55 établit la liste des traitements qui demeurent soumis à une formalité préalable auprès de l'autorité de protection.

Il s'agit tout d'abord de la formalité de demande d'avis concernant trois catégories de traitements qui présentent une sensibilité particulière : d'une part, les traitements de données à caractère personnel mis en œuvre à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces (article 61), d'autre part, les traitements de données à caractère personnel relatifs aux données génétiques ou biométriques (article 74), et enfin, les traitements de données à caractère personnel relatifs à la recherche dans le domaine de la santé (articles 75 et 76).

Il s'agit ensuite de la formalité d'autorisation préalable de l'autorité pour certains transferts de données à caractère personnel (article 94).

La section I porte sur les dispositions communes.

L'article 56 précise notamment le régime applicable aux traitements visés aux articles 61 et 74 du projet de loi, lesquels ne peuvent être mis en œuvre que par les autorités administratives et judiciaires compétentes dans le cadre exclusif des missions qui leur sont légalement conférées.

Désormais, ces traitements sont autorisés par arrêté ministériel ou par arrêté du Secrétaire d'État à la Justice, Directeur des Services Judiciaires, après avis motivé de l'autorité de protection lequel est publié concomitamment afin de garantir une plus grande transparence. Dans certains cas particuliers, à titre exceptionnel pour certains traitements visés à l'article 61 présentant une confidentialité particulière, seul le sens de l'avis est publié afin d'éviter de divulguer le raisonnement qui sous-tend l'avis de l'autorité.

L'avis est rendu dans un délai de deux mois renouvelable une fois sur décision motivée du président de l'autorité.

L'article 57 liste les mentions obligatoires devant être présentes dans la demande d'avis ou la demande d'autorisation pour que celle-ci soit recevable. Cette dernière doit notamment comporter, le fondement juridique du traitement, sa finalité, les catégories de données à caractère personnel concernées, une analyse des risques relative à la sécurité du traitement ainsi que l'autorité auprès de laquelle s'exerce le droit d'accès.

L'article 58 impose de tenir l'autorité de protection informée en cas de changement affectant les informations visées à l'article 57 ou en cas de suppression du traitement.

Afin de garantir une plus grande transparence aux personnes concernées, l'article 59 liste les informations devant figurer obligatoirement dans l'arrêté du Ministre d'État ou du Secrétaire d'État à la Justice, Directeur des Services Judiciaires.

L'article 60 prévoit que l'autorité de protection tient à disposition du public la liste des traitements ayant fait l'objet d'une des formalités prévues à l'article 55.

La section II porte sur les traitements de données à caractère personnel mis en œuvre à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces, visés par la directive (UE) 2016/680.

La protection des personnes physiques à l'égard de ces traitements fait l'objet d'un acte juridique spécifique de l'Union européenne, en l'occurrence la directive susvisée, de sorte que le R.G.P.D. ne s'applique pas aux activités de traitement effectuées à ces fins.

Ces activités sont axées principalement sur la prévention et la détection des infractions pénales et les enquêtes et les poursuites en la matière, y compris les activités de police effectuées sans savoir au préalable si un incident constitue une infraction pénale ou non. Elles peuvent également comprendre, par l'adoption de mesures coercitives, notamment les activités de police lors de manifestations ou de grands événements sportifs. Parmi ces activités figurent également le maintien de l'ordre public, la protection contre les menaces pour la sécurité publique et pour les intérêts fondamentaux de la Principauté et la prévention de telles menaces, qui sont susceptibles de déboucher sur une infraction pénale. Ce périmètre est celui de la présente section. Il apparait beaucoup plus complet que le champ de l'article 11 de la loi n° 1.165 en s'adossant à l'évolution du droit européen en la matière.

La section comporte les 13 articles présentés ci-après.

L'article 61 précise le régime applicable aux traitements relevant de la section II. Il définit ainsi la ligne de partage entre ce qui correspond aux dispositions générales relevant des traitements du R.G.P.D. et à celles relevant de la directive quant à leur champ d'application respectif. De ce fait, les traitements mis en œuvre pour les finalités précisées au premier alinéa de l'article sont régis par les dispositions de la section et, sous réserve de leur compatibilité, par les autres dispositions de la loi.

Le second alinéa précise, quant à lui, le régime de licéité applicable. Pour qu'ils soient licites, ces traitements doivent satisfaire trois conditions cumulatives : d'une part, être mis en œuvre par une autorité compétente, administrative ou judiciaire, dans le cadre exclusif des missions qui leur sont conférées, d'autre part, être fondés sur une base légale, à savoir une disposition législative ou réglementaire et, enfin, être nécessaires à l'une des finalités énoncées à l'alinéa premier.

L'article 62 fixe les conditions dans lesquelles les données collectées au titre de la présente section peuvent faire l'objet d'une réutilisation dans un traitement ne relevant pas du même régime juridique, à savoir soit le régime de droit commun du R.G.P.D, soit le régime prévu à la section VI du Chapitre VII.

Du fait de la sensibilité des données collectées en application de l'article 61, il parait indispensable qu'une éventuelle réutilisation de ces données ne puisse être faite que sur la base d'un fondement légal, ou en exécution d'engagements internationaux de la Principauté. Il en est ainsi par exemple des responsables du traitement visés à l'article 77, lesquels sont habilités, sous certaines conditions, à mettre en œuvre un traitement relatif à des infractions ou condamnations pénales.

L'article 63 prévoit la possibilité de réaliser de nouveaux traitements à partir de la collecte initiale de données sous la triple condition suivante : que le responsable du traitement soit autorisé à traiter ces données, que la nouvelle finalité s'inscrive dans celles énoncées à l'article 61 et enfin que les nouveaux traitements soient nécessaires et proportionnés à la nouvelle finalité.

Il pourrait s'agir par exemple, à partir d'un traitement d'antécédents judiciaires, de la possibilité de créer un nouveau traitement concernant des catégories d'auteurs particuliers, tels que les auteurs de violences conjugales ou encore de créer un fichier d'interdits de stade.

Les traitements ultérieurs à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique, statistique ou historique sont par ailleurs compatibles, sous réserves de garanties appropriées.

Des garanties appropriées doivent être prises par le responsable du traitement afin de s'assurer que les traitements respectent les principes fondamentaux de licéité, de loyauté et de transparence, de limitation des finalités, de minimisation des données, d'exactitude, de limitation de la conservation, de l'intégrité et de la confidentialité des données et de responsabilité du responsable du traitement.

L'article 64 porte sur le profilage et la décision individuelle automatisée dans le cadre spécifique des traitements relevant des finalités visées à l'article 61. Si ces procédés peuvent être utilisés dans de nombreux secteurs, y compris pour des activités relevant des autorités administratives et judiciaires compétentes, ils sont susceptibles de présenter des risques significatifs pour les droits et libertés des personnes concernées et nécessitent donc des garanties appropriées.

Il est ainsi précisé que la « *prise de décision exclusivement automatisée »* est la capacité de prendre des décisions par des moyens technologiques sans intervention humaine dans le processus décisionnel.

Conformément aux dispositions de la directive, le projet de loi interdit ce type de décision y compris le profilage, lorsqu'elle produit des effets juridiques défavorables pour la personne concernée ou l'affecte de manière significative, comme par exemple l'application de mesures de sécurité ou de surveillance accrue de la personne concernée. Une telle décision peut toutefois être autorisée par arrêté ministériel ou par arrêté du Secrétaire d'Etat à la Justice, Directeur des Services Judiciaires. Dans ce cas, le responsable du traitement fournit des garanties appropriées pour les droits et libertés de la personne concernée, telles que le droit d'obtenir une intervention humaine, d'exprimer son point de vue ou d'obtenir une explication quant à la décision prise ou de la contester.

Est également interdit tout profilage entraînant une discrimination sur la base de données sensibles.

L'article 65 impose au responsable du traitement de prendre les mesures raisonnables pour respecter le principe d'exactitude des données consacré par la loi.

Sont considérées comme raisonnables les mesures qui ne nécessitent pas, de la part du responsable du traitement, un investissement ou un effort disproportionné, c'est-à-dire tenant compte des moyens dont il dispose. En cas de transmission des données, l'information du destinataire est prévue de manière à assurer l'exactitude des données et de permettre leur rectification ou leur effacement en cas de transmission illicite.

L'article 66 énonce les différentes catégories de personnes devant être distinguées par le responsable du traitement, au moment de la collecte des données.

En effet, le traitement des données dans les domaines particuliers de la présente section implique nécessairement que soient traitées des données concernant différentes catégories de personnes concernées, par exemple les personnes reconnues coupables d'une infraction pénale, les victimes et les autres parties, telles que les témoins, les personnes détenant des informations, les contacts ou les associés des personnes soupçonnées ou condamnées. La directive 2016/680 prévoit qu'il importe dès lors d'établir une distinction claire, le cas échéant et dans la mesure du possible, entre les données à caractère personnel des différentes catégories de personnes concernées.

C'est à cet objectif que répond le présent article.

L'article 67 impose au responsable du traitement ou à son sous-traitant d'établir un journal des opérations réalisées, permettant de retracer par exemple l'heure, la date ou le motif d'une consultation des données d'un traitement. Le journal des opérations est un outil essentiel de contrôle de la protection des données en ce qu'il permet de vérifier la pertinence des opérations et de suivre l'activité des utilisateurs afin de détecter d'éventuelles utilisations abusives.

Il est mis à la disposition de l'autorité de protection à sa demande.

L'article 68 est relatif à l'exercice des droits. Il prévoit que le responsable du traitement prend les mesures raisonnables pour fournir toute information et procéder à toute mesure relative à l'exercice des droits de la personne concernée de façon concise, compréhensible et aisément accessible. Les informations sont fournies gratuitement par tout moyen approprié. Il informe la personne concernée des suites données à sa demande dans les meilleurs délais.

L'article 69 porte sur les informations que le responsable du traitement met à disposition de la personne concernée et en dresse la liste. Cet article est dérogatoire au droit d'information général issu du Règlement européen en ce que le responsable du traitement peut retarder, limiter ou ne pas fournir lesdites informations, lorsque leur communication risquerait de porter atteinte aux enquêtes, recherches ou procédures officielles ou judiciaires en cours, à la prévention ou à la détection d'infractions pénales, aux enquêtes ou aux poursuites en la matière ou à l'exécution de sanctions pénales, à la sécurité publique ou à la sécurité nationale ou pour protéger les droits et liberté d'autrui.

L'article 70 prévoit une dérogation à la communication d'une violation de données à caractère personnel à la personne concernée. En effet, conformément aux dispositions prévues par la directive (UE) 2016/680 cette communication peut être retardée, limitée ou ne pas être délivrée par le responsable du traitement pour éviter de gêner des enquêtes, des recherches ou des procédures administratives ou judiciaires, pour éviter de nuire à la prévention ou à la détection d'infractions pénales, aux enquêtes ou aux poursuites en la matière ou à l'exécution de sanctions pénales, pour protéger la sécurité publique, pour protéger la sécurité nationale ou pour protéger les droits et libertés d'autrui.

L'article 71 institue un droit d'accès indirect auprès de l'autorité de protection, dans le prolongement de la procédure déjà créée par la loi n° 1.165 du 23 décembre 1993, modifiée, précitée.

Avec l'accord du responsable du traitement, le président de l'autorité de protection peut ainsi porter à la connaissance de la personne concernée les informations dont la communication ne porte pas atteinte aux enquêtes ou procédures judiciaires en cours, à la sécurité publique ou à la préservation de la sécurité nationale.

En cas de refus de communication pour les motifs susvisés, l'autorité de protection indique à la personne concernée ses voies de recours.

L'article 72 est relatif aux droits de rectification et d'effacement. Il confère aux personnes physiques le droit de faire rectifier les données à caractère personnel les concernant ou de les faire effacer si celles-ci s'avèrent inexactes ou manifestement erronées. À l'appui de sa demande, la personne concernée doit produire toutes les pièces justificatives utiles auprès du responsable du traitement.

Ce dernier peut refuser une demande de rectification ou d'effacement si celle-ci est de nature à porter atteinte aux enquêtes ou procédures judiciaires en cours, à la sécurité publique ou à la préservation de la sécurité nationale.

L'article 73 définit le cadre juridique applicable aux transferts des données hors de la Principauté lorsqu'elles portent sur des traitements relevant de l'article 61. Ce régime diffère du régime de droit commun des transferts prévus aux articles 93 à 95 du projet de loi dans la mesure où les conditions de transfert ne sont pas forcément adaptées aux traitements mis en œuvre à des fins de « Police-Justice ». Ces conditions sont également applicables aux transferts de données relevant des traitements de sécurité nationale mis en œuvre au titre des articles 9 à 15 et 18 de la loi n° 1.430, précitée.

Le chiffre 1 opère un renvoi à l'article 93 et pose le principe que le transfert ne peut s'opérer qui si l'Etat ou l'organisation internationale présente un niveau de protection adéquat constaté par la Principauté. Pour cette catégorie de traitements, le niveau de protection s'entend au titre de la directive (UE) 2016/680. En l'absence d'un tel niveau de protection, le transfert peut être réalisé lorsque des garanties appropriées sont offertes dans un instrument juridiquement contraignant assurant la protection des données à caractère personnel, ou lorsque l'évaluation de toutes les circonstances entourant le transfert permet d'estimer qu'il existe des garanties appropriées en matière de protection des données à caractère personnel. Cet instrument juridiquement contraignant peut être un accord bilatéral conclu avec l'Etat ou l'organisation internationale destinataire et mis en œuvre par la Principauté dans son ordre juridique qui respecte les exigences en matière de protection des données et les droits des personnes concernées, y compris le droit à un recours administratif ou juridictionnel effectif s'agissant des transferts de données traitées pour l'une des finalités de l'article 61.

Lorsqu'il évalue toutes les circonstances entourant le transfert de données, le responsable du traitement prend en compte le fait que le transfert sera soumis à des obligations de confidentialité et au principe de spécificité, ce qui garantit que les données ne seront pas traitées à des fins autres que celles pour lesquelles elles ont été transférées.

Comme le permet la directive (UE) 2016/680, le chiffre 2 prévoit des dérogations en l'absence d'adéquation ou de garanties appropriées parmi lesquelles la prévention d'une menace grave et immédiate pour la sécurité publique ou pour préserver les intérêts fondamentaux de l'Etat.

Le chiffre 3 donne la possibilité de limiter un transfert de données malgré une décision d'adéquation ou des garanties appropriées pour des motifs importants d'intérêt public. Par le biais de cette disposition, conforme à la Convention 108+, le projet de loi se veut particulièrement protecteur à l'égard des droits et libertés de la personne concernée.

Le chiffre 4 énonce les deux exigences qui sont requises par la directive (UE) 2016/680 pour ces catégories de transferts : d'une part, le transfert doit être effectué auprès d'une autorité publique compétente, c'est-à-dire habilitée à recevoir les données et, d'autre part, il doit être nécessaire à l'une des finalités énoncées à l'article 61.

Les chiffres 5 et 6 sont relatifs aux transferts ultérieurs de données. Un transfert de données provenant d'un autre État ne peut s'effectuer que si cet État a préalablement autorisé le transfert. Une telle mesure vise à assurer aux États communiquant leurs données aux autorités compétentes monégasques qu'il ne sera pas réalisé de transfert ultérieur de données compromettant le niveau de protection qui y est attaché. Lorsque le caractère immédiat de la menace pour la sécurité publique rend impossible l'obtention d'une autorisation préalable en temps utile et afin d'assurer une coopération efficace en matière répressive, ces dispositions permettent à l'autorité compétente de transférer les données à caractère personnel vers un pays ou une organisation internationale sans l'obtention de cette autorisation au regard de facteurs pertinents.

La section III concerne les traitements de données biométriques et génétiques nécessaires à l'authentification ou au contrôle de l'identité d'une personne.

L'article 74 définit le régime juridique applicable aux traitements de données biométriques ou génétiques nécessaires à l'authentification ou au contrôle de l'identité d'une personne unique lorsqu'ils sont mis en œuvre par une autorité publique, et plus précisément par une autorité administrative ou judiciaire agissant dans l'exercice de ses prérogatives de puissance publique. Il peut s'agir, par exemple, d'un traitement mis en œuvre pour la délivrance de passeports ou de cartes d'identité qui nécessite la collecte de données biométriques ou encore de traitements mis en œuvre à des fins de police scientifique.

Pour ces catégories de traitements, le Gouvernement a souhaité conserver le régime de consultation préalable de l'autorité eu égard au caractère sensible des données utilisées et à l'enjeu de protection de la vie privée. Lorsque l'Etat n'agit pas dans le cadre de ses prérogatives de puissance publique mais comme un employeur par exemple, pour contrôler l'accès aux locaux de ses services, une demande d'avis n'est pas requise. En revanche, il demeure soumis, à l'instar d'un responsable du traitement du secteur privé, à une analyse d'impact en cas de traitement à grande échelle de données sensibles.

Le deuxième alinéa de l'article 74 prévoit que le responsable du traitement adopte des garanties appropriées spécifiques pour les droits et libertés notamment en ce qui concerne la conservation ou la transmission de ces données.

Le troisième alinéa précise que lorsque le traitement de données biométriques ou génétiques est mis en œuvre pour l'une des finalités énoncées à l'article 61, à savoir les finalités de la directive (UE) 2016/680, le régime de transfert applicable à ces données est celui prévu pour les traitements de ladite directive par renvoi aux dispositions de l'article 73.

La section IV comprend deux articles qui concernent les traitements de données à caractère personnel relatifs à la recherche dans le domaine de la santé.

L'article 75 soumet à l'avis motivé de l'autorité de protection la mise en œuvre des traitements de données à caractère personnel ayant pour finalité la recherche dans le domaine de la santé. Préalablement au prononcé de cet avis, l'autorité de protection peut, dans des conditions fixées par ordonnance souveraine, consulter un service public compétent dans le domaine de la santé.

Cette disposition harmonise la procédure de mise en œuvre, qui est désormais commune au secteur privé et au secteur public, dans le cadre de la recherche dans le domaine de la santé.

L'article 76 prévoit qu'en ce qui concerne les traitements effectués dans le cadre d'une recherche impliquant la personne humaine, le dossier produit à l'appui de la demande d'avis comporte, en sus des éléments prévus à l'article 57, la mention de l'objectif de la recherche, de la population concernée, de la méthode d'observation ou d'investigation retenue, de la justification du recours aux données à caractère personnel traitées, de la durée et des modalités d'organisation de la recherche, de la méthode d'analyse des données, ainsi que, le cas échéant, une copie de l'avis émis par le comité compétent en application de la législation mentionnée à l'alinéa précédent. Il est à noter que l'autorité de protection n'est pas compétente pour apprécier la qualification d'une recherche impliquant la personne humaine.

Le Chapitre VII établit des dispositions particulières s'appliquant à certaines catégories de traitements. Il comporte six sections.

La section I est dédiée aux traitements de données à caractère personnel relatifs aux infractions, aux condamnations pénales et mesures de sûreté ou portant sur des soupçons d'activités illicites et découle directement de l'article 10 du R.G.P.D.

L'article 77 dresse la liste des personnes pouvant mettre en œuvre, sous réserve de garanties appropriées, des traitements de données à caractère personnel entrant dans ce qui correspond au champ d'application de la directive « *Police-Justice* », à savoir relatifs aux infractions, aux condamnations pénales et mesures de sûreté ou portant sur des soupçons d'activités illicites dans le cadre de leurs activités.

En plus des autorités administratives et judiciaires compétentes visées à l'article 56, sont également concernées d'autres catégories de personnes ou d'entités, notamment les personnes morales de droit privé collaborant au service public de la justice ou agissant dans le cadre de leurs obligations légales, les associations d'aide aux victimes ou encore les établissements bancaires pour leurs obligations de lutte contre la fraude et le blanchiment.

La section II est relative aux traitements à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques.

Comme précisé ci-avant, il s'agit de traitements mis en œuvre par les autorités ayant une obligation légale de collecte et de conservation d'archives définitives, à savoir aujourd'hui, le Service central des archives et de la documentation administrative et la Mairie. Ces traitements bénéficient d'un statut particulier dérogatoire au régime de droit commun en ce qui concerne l'exercice de certains droits selon que les traitements sont réalisés à des fins archivistiques dans l'intérêt public ou à des fins de recherche scientifique ou historique ou à des fins statistiques. En contrepartie de ce régime spécifique, des garanties appropriées sont requises. Il peut s'agir de la pseudonymisation des données ou encore de la mise en place de mesures techniques et organisationnelles appropriées. Tel est le sens du premier alinéa de l'article 78 pour la mise en œuvre de ces traitements.

Le deuxième alinéa précise les dérogations applicables aux traitements à des fins archivistiques dans l'intérêt public tandis que le troisième alinéa prévoit celles applicables aux traitements mis en œuvre à des fins de recherche scientifique ou historique ou à des fins statistiques.

Ces dérogations sont distinctes mais portent notamment sur les droits d'accès, de rectification et d'opposition dans la mesure où l'exercice de ces droits risquerait de rendre impossible ou d'entraver la réalisation des finalités pour lesquelles les données à caractère personnel sont collectées.

L'article 78 précise également que les archives du secteur privé ne peuvent bénéficier des dérogations associées aux traitements à des fins archivistiques dans l'intérêt public mais qu'elles peuvent s'en prévaloir lorsque le traitement a également pour finalité la recherche historique.

La section III concerne les traitements relatifs à la liberté d'expression.

L'article 79 permet de concilier la protection des données à caractère personnel et la liberté d'expression et ainsi d'assurer un équilibre entre les droits à l'égard de leur données et ladite liberté d'expression consacrée notamment tant par l'article 10 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (C.E.D.H.) que par la loi n° 1.299 du 15 juillet 2005 sur la liberté d'expression publique, modifiée.

Ainsi, comme le prévoient le R.G.P.D. et la Convention 108+, cet article comporte des dérogations pour les catégories de traitements mis en œuvre à des fins journalistiques et à des fins d'expression incluant l'expression universitaire, artistique ou littéraire. Elles touchent à la conservation des données, aux données sensibles ainsi qu'aux droits des personnes et aux transferts.

La section IV concerne les traitements relatifs à la vidéosurveillance.

En consacrant une section aux traitements relatifs à la vidéosurveillance, le projet de loi entend apporter une attention particulière à cette catégorie de traitements de données à caractère personnel, qu'il s'agisse de systèmes d'enregistrement et de conservation des images ou de systèmes de surveillance en temps réel, sans enregistrement, de tels traitements pouvant potentiellement présenter des risques pour la protection de la vie privée.

Dès lors que sont exclus du champ d'application de la présente loi les traitements de données effectués dans le cadre d'activités exclusivement personnelles ou domestiques, l'exploitation d'un système de caméra donnant lieu à un enregistrement vidéo par un particulier à son domicile afin de protéger les biens et assurer la sécurité des personnes qui y vivent n'entre pas dans le champ des dispositions de la présente section. Pour autant, le dispositif doit respecter la vie privée des voisins ou des visiteurs.

Si le dispositif de vidéosurveillance est utilisé en dehors de la sphère strictement privée, c'est-à-dire lorsque des personnes extérieures au cercle familial ou amical interviennent au domicile comme par exemple, des gens de maisons ou des aides à domicile, le particulier en tant qu'employeur doit respecter les dispositions de la présente section.

Les traitements de vidéosurveillance se distinguent des traitements de vidéoprotection prévus par la loi n° 1.430 du 13 juillet 2016, précitée, lesquels sont destinés à assurer la protection des bâtiments et installations publiques, la prévention des atteintes à la sécurité des biens et des personnes, la prévention des actes de terrorisme ou d'atteinte aux intérêts fondamentaux de la Principauté. Pour ces raisons, ils ne peuvent être mis en œuvre que par les autorités administratives compétentes, notamment le Directeur de la Sûreté Publique.

Ainsi, le respect des dispositions de la présente loi ne nécessitera plus l'obtention, pour les personnes privées et publiques autres que celles visées par la loi n° 1.430 du 13 juillet 2016, précitée, de l'autorisation d'exploiter un système de vidéosurveillance sur le fondement de la loi n° 1.264 du 23 décembre 2002 relative aux activités privées de protection des personnes et des biens, ni l'autorisation de l'autorité de protection, conséquence directe de la suppression de la plupart des formalités préalables.

En contrepartie, le responsable du traitement devra scrupuleusement respecter les principes de protection et les obligations prévus par la présente loi, à savoir les principes de licéité du traitement, de finalité, de transparence et de proportionnalité.

Il devra également, dans certains cas, tenir un registre ou procéder à une analyse d'impact comme notamment lorsque la surveillance s'exerce à grande échelle, par exemple, dans un centre commercial ou dans une galerie marchande, conformément aux dispositions de l'article 32 relatif à l'analyse d'impact.

L'article 80 pose le principe de la liberté d'installer un système de vidéosurveillance dans des lieux ouverts ou non au public dès lors que le système a pour finalité la sécurité des biens et des personnes.

De fait, sont concernés les lieux ouverts au public tels qu'un restaurant, une galerie commerciale ou un guichet d'administration ainsi que les lieux non ouverts au public, comme par exemple un lieu privé (domicile, garage…) ou des locaux à usage professionnel tels que les bureaux ou les entrepôts. Par souci de clarté, l'article définit également la vidéosurveillance.

L'article 81 énonce les obligations incombant au responsable du traitement en matière d'information des personnes de la présence d'un système de vidéosurveillance. Cette information est différente selon qu'il s'agit d'un lieu ouvert ou non au public.

S'il s'agit d'un lieu ouvert au public, l'information est réalisée par le responsable du traitement de façon visible et permanente au moyen d'un panneau placé à l'extérieur des lieux surveillés qui doit comporter au minimum les informations relatives aux finalités du traitement, à l'identité du responsable du traitement et à l'exercice des droits de la personne concernée.

S'il s'agit d'un lieu non ouvert au public, comme par exemple les lieux de travail, l'information doit être réalisée par le responsable du traitement de manière identique au moyen d'un panneau placé à l'intérieur des lieux concernés. Cette information peut être également donnée à la personne concernée par une information appropriée lorsqu'il s'agit, par exemple, d'employeurs de gens de maison.

Il est également précisé que la durée de conservation des images issues des systèmes de vidéosurveillance ne doit pas excéder trente jours.

L'article 82 soumet à l'autorisation préalable du Ministre d'État l'installation d'un système de vidéosurveillance dans des lieux ouverts au public ou lorsque le système filme les abords de voies publiques ou d'espaces ouverts au public ou à la circulation du public.

L'arrêté ministériel pris en application de cette section précisera les conditions de délivrance de cette autorisation.

Par ailleurs, afin que l'autorité de protection puisse être pleinement informée des dispositifs de vidéosurveillance mis en place en Principauté dans les lieux non ouverts au public et exercer sa mission de contrôle, le responsable du traitement doit tenir informée l'autorité de protection de la présence de cette installation.

Enfin, l'article 83 dispose que les modalités d'application de la présente section sont définies par arrêté ministériel.

La section V concerne les traitements de données à caractère personnel dans le secteur des communications électroniques.

L'article 84 reprend les dispositions de l'article 14.2 de la loi n° 1.165 du 23 décembre 1993, modifiée, précitée. Il impose aux opérateurs de communications électroniques de délivrer à l'utilisateur ou l'abonné, une information préalable à la mise en œuvre des traitements utilisés pour accéder ou collecter les données à caractère personnel conservées dans son équipement terminal.

Le dernier alinéa de l'article 84 interdit aux opérateurs de communications électroniques de subordonner l'accès à un service disponible sur un réseau de communications électroniques à l'acceptation du traitement des données stockées sur l'équipement terminal de l'utilisateur ou l'abonné. Un tel comportement est accepté uniquement si le traitement des données stockées sur l'équipement terminal de la personne concernée permet exclusivement d'effectuer ou de faciliter la transmission d'une communication ou est strictement nécessaire à la fourniture d'un service expressément demandé par la personne concernée.

La section VI concerne les traitements mis en œuvre dans le cadre des dispositions des articles 9 à 15 et 18 de la loi n°1.430 du 13 juillet 2016 portant diverses mesures relatives à la préservation de la sécurité nationale. Elle comporte les huit articles présentés ci-après.

Afin de renforcer l'indépendance fonctionnelle de la Commission de l'article 16 au regard de son indépendance, l'article 85 a pour objet de modifier le quatrième alinéa de l'article 16 de la loi n° 1.430 du 13 juillet 2016, précitée, afin de porter de un à cinq ans la durée des mandats des membres proposés par le Conseil National et le Conseil d'Etat.

L'article 86 a pour objet de conférer une nouvelle compétence à la Commission de l'article 16 créée par la loi précitée qui est l'autorité de protection spécifiquement désignée. Celle-ci est chargée de contrôler, en toute indépendance, les traitements mis en œuvre dans le cadre des dispositions des articles 9 à 15 et 18 de ladite loi, qui sont liés aux activités de renseignement et aux techniques spéciales d'investigation. Le contrôle de la Commission concerne les dispositions de la loi n° 1.430 du 13 juillet 2016, précitée, et celles de la présente loi applicables à ces traitements.

La création de ce mécanisme de supervision répond à l'exigence de la Convention 108+ de soumettre les activités de traitement à des fins de sécurité nationale à un contrôle indépendant effectif, ce qui apparait particulièrement protecteur par comparaison à d'autres mécanismes mis en place par certains Etats.

L'article 87 précise le régime applicable aux traitements relevant de cette section.

Le premier alinéa de cet article définit le champ d'application de la section VI et fixe le cadre législatif complet applicable aux traitements considérés par référence au chiffre 2 du quatrième alinéa de l'article 34. Il s'agit, comme pour les traitements relevant de la directive « *Police-justice* », de définir la ligne de partage entre les dispositions générales applicables à ces traitements et celles plus spécifiques liées à leurs finalités. Ainsi, les traitements mis en œuvre pour les finalités visées au chiffre 2 du quatrième alinéa de l'article 34 sont régis par les dispositions de la présente section VI et, sous réserve de leur compatibilité avec ces dernières, par les autres dispositions de la loi.

Le second alinéa précise le régime de licéité applicable à ces traitements. Ce régime est spécifique parce qu'il permet, eu égard à leur nature, de déroger à certaines dispositions en matière de protection des données, comme le prévoit l'article 11 de la Convention 108+ lorsque la protection de la sécurité nationale est en jeu.

L'article 88 soumet cette catégorie de traitements à une demande d'avis auprès de la Commission de l'article 16 et définit la procédure de saisine.

En faisant ce choix, le Gouvernement entend apporter un encadrement particulièrement protecteur des données personnelles en imposant une formalité de consultation qui ne résulte ni de la Convention 108+ ni du paquet européen des données.

Le dossier de demande d'avis communiqué à la Commission devra comporter l'ensemble des mentions prévues à l'article 57 de la présente loi, notamment celles portant sur les catégories de données personnelles, la durée de conservation ainsi que l'analyse de risques.

Les traitements sont autorisés par un arrêté ministériel, lequel est dispensé de publication au Journal de Monaco, eu égard à la confidentialité des informations qui font l'objet d'une mesure de classification en application de l'article 18 de la loi n° 1.430 du 13 juillet 2016, précitée.

L'article 89 organise le contrôle de la Commission sur ces traitements en précisant qu'elle peut accéder aux données sous réserve des nécessités de la protection des sources et de la protection des données communiquées par les services de renseignements étrangers. Il donne par ailleurs pouvoir au président de la Commission de saisir le Ministre d'Etat en cas d'irrégularité constatée pour qu'il prenne toutes mesures afin de faire cesser lesdites irrégularités ou pour que leurs effets soient supprimés.

Par ailleurs, pour satisfaire l'obligation de sensibilisation à la protection des données prévue par la Convention 108+, la Commission peut, sous réserve des dispositions relatives au secret de sécurité nationale, rendre compte publiquement et périodiquement de ses activités de contrôle au titre de la présente loi.

L'article 90 prévoit l'exercice d'un droit d'accès, de rectification et d'effacement qui s'exerce auprès de la Commission de l'article 16 selon une procédure spécifique.

Si la Commission considère qu'il peut être fait droit à la demande de rectification ou d'effacement, le président de la Commission saisit le Ministre d'Etat afin qu'il prenne toutes mesures pour y procéder.

A l'issue de cette procédure, la Commission notifie à la personne concernée que les vérifications ont été effectuées. Cependant, eu égard à la nécessaire protection du secret de sécurité nationale, la Commission ne peut confirmer ou infirmer la mise en œuvre de l'une des opérations de police administrative visées par les articles 9 à 15 de la loi n° 1.430 du 13 juillet 2016, précitée, ou l'existence de données la concernant dans un traitement institué dans le cadre de l'article 18 de cette loi. Telle est la formulation également utilisée par la formation spécialisée du Conseil d'Etat français dans une situation analogue.

A cet égard, il convient de préciser que la Cour Européenne des Droits de l'Homme est venue rappeler, dans l'affaire Kennedy c. Royaume-Uni, requête n° *26839/05* en date du 18 mai 2010 (§167), que lorsque le justiciable n'est pas informé de l'existence d'une mesure de surveillance qui le concerne, il importe que la juridiction ou la commission chargée du contrôle remplisse les critères suivants *: « être un organe indépendant et impartial, qui a édicté son propre règlement de procédure et dont les membres exercent ou ont exercé de hautes fonctions judiciaires ou sont des juristes chevronnés. Lorsqu'elle examine les griefs d'un justiciable, la juridiction devrait avoir accès à toutes les informations pertinentes, y compris les informations confidentielles* », critères auxquels répond la Commission de l'article 16.

L'article 91 concerne les transferts de données à caractère personnel relatifs aux traitements de sécurité nationale mis en œuvre au titre des articles 9 à 15 et 18 de la loi n° 1.430 du 13 juillet 2016, précitée. En faisant référence aux dispositions de l'article 73, c'est-à-dire celles applicables aux traitements relevant de la directive « *Police-Justice* », le Gouvernement garantit un niveau de sécurité élevé de protection de la vie privée en fondant le transfert par référence à une protection adéquate, du pays ou de l'organisation internationale destinataire, tandis que certains Etats requièrent un niveau « *suffisant* » de protection.

A l'instar de l'article 85, l'article 92 a pour enjeu de renforcer l'indépendance fonctionnelle de la Commission de l'article 16 en prévoyant que les crédits nécessaires à son fonctionnement sont inscrits dans un chapitre spécifique du budget de l'Etat.

Le Chapitre VIII prévoit les conditions dans lesquelles peuvent s'effectuer des transferts de données à caractère personnel hors de la Principauté.

Un transfert de données intervient lorsque des données à caractère personnel sont communiquées ou mises à disposition d'un destinataire situé à l'extérieur de la Principauté. Dès lors que les données sont rendues accessibles, même au moyen d'un simple accès à distance, il y a transfert de données.

La libre circulation de l'information sans considération des frontières constitue un enjeu majeur dans le contexte de la mondialisation des échanges. La Convention 108+ du Conseil de l'Europe, le R.G.P.D. et la directive (UE) 2016/680 s'accordent à considérer qu'il y a lieu de faciliter cette libre circulation dès lors qu'une protection appropriée des personnes à l'égard du traitement des données est assurée. Le projet de loi s'inscrit dans cette démarche en recherchant un juste équilibre entre la nécessaire circulation des données dans une économie de plus en plus numérique et mondialisée et le respect des droits et libertés fondamentaux des individus.

Ce sont les entités transférant les données, en général les responsables du traitement, qui doivent s'assurer de la mise en place de mécanismes encadrant ces transferts. Lors d'un transfert, le responsable du traitement doit tenir compte de plusieurs éléments parmi lesquels la nature des données, les finalités et la durée des traitements pour lesquels les données sont transférées, le respect de la prééminence du droit par le pays de destination finale, les règles de droit, générales et sectorielles applicables dans l'État ou l'organisation en question ainsi que les règles professionnelles et de sécurité qui y sont respectées.

Le Chapitre VIII est composé de cinq articles qui recouvrent des situations différentes de transfert de données à caractère personnelles hors de la Principauté.

L'article 93 pose le principe selon lequel tout transfert de données personnelles hors de la Principauté peut s'effectuer si la législation ou la réglementation des données personnelles d'un Etat ou de l'organisation internationale destinataire présente un niveau de protection adéquat constaté par la Principauté.

Il s'agit pour le Gouvernement, à l'instar d'autres Etats comme la Suisse et le Royaume-Uni, d'apprécier souverainement vers quels Etats ou organismes internationaux les données peuvent être transférées hors des frontières monégasques sans que le responsable du traitement n'ait à justifier de garanties appropriées complémentaires.

Le niveau de protection adéquat est constaté sur la base d'un ensemble d'éléments, en particulier de l'existence et de la portée d'une décision d'adéquation de la Commission européenne en matière de protection des données. L'adhésion de l'État ou de l'organisation internationale à la Convention 108 concourt à cette appréciation, notamment en cas de ratification du Protocole d'amendement STCE n° 223 modernisant ladite Convention. Selon le rapport explicatif de la Convention 108+, toutes les Parties ayant souscrit au socle commun des dispositions en matière de protection des données de la Convention sont en mesure d'offrir un niveau de protection considéré comme approprié, permettant ainsi en principe la libre circulation des données. Existe toutefois, dans certaines hypothèses, un risque réel et sérieux que cette libre circulation des données à caractère personnel puisse entraîner le contournement des dispositions de la Convention.

Dans ce contexte, l'examen des règles de droit en vigueur dans l'Etat ou l'organisation internationale destinataire constitue un élément sur lequel pourra se fonder le Gouvernement pour constater le niveau de protection des données qui doit être au moins équivalent à celui prévu par le présent projet de loi.

Un arrêté ministériel, pris après avis de l'autorité de protection, déterminera la liste de ces Etats et organisations internationales.

L'article 94 énonce les garanties appropriées qui permettent à un responsable du traitement ou à un sous-traitant d'effectuer un transfert si l'État ou l'organisation internationale destinataire n'assure pas le niveau de protection requis au titre de l'article 93.

Il pourra s'agir notamment du respect d'un engagement international exécutoire dans la Principauté, de l'utilisation de clauses types de protection ou encore d'un mécanisme de certification préalablement approuvé par l'autorité de protection.

L'article 95 prévoit des dérogations pour des situations particulières visées par le R.G.P.D. et la Convention 108+ permettant le transfert de données dans l'hypothèse où les conditions requises au titre des articles 93 et 94 ne sont pas remplies. Ces dérogations permettent d'éviter des situations de blocage de flux transfrontières tout en respectant les droits des personnes concernées.

Ainsi, le transfert pourra être réalisé si la personne concernée y a explicitement consenti, si le transfert est nécessaire pour des motifs importants d'intérêt public ou encore pour l'exécution d'un contrat auquel la personne concernée est partie. D'autres cas sont limitativement prévus. Ainsi, un transfert hors de la Principauté peut également avoir lieu s'il ne revêt pas de caractère répétitif, s'il ne touche qu'un nombre limité de personnes, s'il est nécessaire aux fins d'intérêts légitimes impérieux poursuivis par le responsable du traitement et que des garanties appropriées ont été prises. Dans cette hypothèse, le responsable du traitement doit tenir informée l'autorité de protection de ce transfert.

Enfin, comme le permet la Convention 108+, le chiffre 4 de l'article 95 prévoit la possibilité qu'un transfert de catégories spécifiques de données puisse être limité pour des motifs importants d'intérêt public, notamment pour des raisons de sécurité nationale ou de sécurité publique.

Lorsque le transfert de données ne répond pas aux exigences des articles 93, 94 et 95, le transfert est soumis à l'autorisation préalable de l'autorité de protection comme le prévoit l'article 96.

Enfin, l'article 97 introduit une disposition équivalente à celle de l'article 48 du R.G.P.D. qui porte sur les demandes de transferts ou de divulgation de données à caractère personnel émanant d'une juridiction ou d'une autorité administrative d'un pays tiers à l'Union européenne. Il prévoit que la demande émanant d'une telle autorité ne constitue pas en elle-même un motif légitime de transfert, encore faut-il qu'elle soit fondée sur un accord international en vigueur entre le pays tiers et le pays membre de l'Union européenne.

En intégrant une disposition équivalente dans le projet de loi, le Gouvernement a souhaité encadrer la situation dans laquelle une entreprise monégasque pourrait être requise par un Etat étranger aux fins de divulgation ou de transfert de données, c'est-à-dire un transfert non pas voulu par elle mais qui lui est autoritairement demandé. Dans ce cas, l'entreprise monégasque pourrait invoquer les dispositions de la loi en s'assurant au préalable que la réquisition est bien prise sur le fondement d'un traité international. Si tel n'est pas le cas, en faisant droit à cette réquisition, l'entreprise serait en non-conformité avec la loi monégasque et s'exposerait ainsi aux sanctions qu'elle prévoit.

Le Chapitre IX porte sur la compétence juridictionnelle, les sanctions pénales et le droit à réparation.

Les articles 98 et 99 prévoient les règles de compétence internationale applicables en matière de protection des données et la possibilité, pour la personne concernée, d'être représentée par un organisme, une organisation ou une association autorisés ou reconnus à Monaco pour exercer en son nom un recours juridictionnel.

Les sanctions pénales énoncées par l'article 100 reprennent, en partie, celles prévues aux articles 21 et 22 de la loi n °1.165 du 23 décembre 1993, modifiée, précitée. Le projet de loi tend à assurer un équilibre des sanctions entre les manquements relevant de la compétence de la formation restreinte de l'autorité de protection, notamment par le prononcé d'amendes financières, et ceux dont le degré de gravité justifie de les qualifier d'infractions pénales.

Au titre des nouvelles infractions pénales peuvent être cités l'absence de tenue d'un registre des activités de traitements lorsque celui-ci est rendu obligatoire en vertu des dispositions de l'article 26, le non-respect de la protection des données dès la conception et par défaut et le non-respect de la notification d'une violation de données à la personne concernée.
L'article 100 précise également que les sanctions pénales ne sont pas applicables à l'État, à la Commune et aux établissements publics conformément aux dispositions de l'article 4-4 du Code pénal.

L'article 101 relatif aux effets de la condamnation pénale conserve la rédaction issue de l'article 23 de la loi n° 1.165 du 23 décembre 1993, modifiée, précitée. Les effets de la condamnation sont uniquement adaptés aux nouvelles obligations des acteurs. Ainsi, toute condamnation entraîne la suppression des traitements et non plus la cessation des effets de la déclaration ou de l'autorisation et la radiation du répertoire des traitements automatisés.

L'article 102 instaure un droit à réparation non explicitement prévu par la loi n° 1.165 du 23 décembre 1993, modifiée, précitée, mais découlant du premier paragraphe de l'article 82 du R.G.P.D. Cet article traite de la responsabilité civile du responsable du traitement et du sous-traitant qui devront indemniser toute personne ayant subi un dommage matériel ou moral du fait de leur violation de la présente loi. L'objectif de la mise en place d'une telle responsabilité est d'impliquer les responsables du traitement et sous-traitants au respect de leurs obligations.

Le Chapitre X comporte les dispositions finales permettant d'organiser la mise en œuvre de la nouvelle loi relative à la protection des données.

L'article 103 prévoit que l'Autorité de Protection des Données Personnelles succède à la Commission de Contrôle des Informations Nominatives en tous ses droits et obligations, par exemple en matière de contrats de personnel ou de location des locaux.

L'article 104 permet aux membres de la C.C.I.N. de rester en fonction jusqu'à la nomination des membres de la nouvelle autorité de protection auxquels s'applique un nouveau mandat de cinq ans renouvelable une fois.

L'article 105 prévoit des dispositions transitoires et décrit trois situations de mise en conformité des traitements.

La première concerne les responsables du traitement à qui un délai d'un an est accordé à compter de l'entrée en vigueur de la présente loi pour mettre leur traitement en conformité avec les dispositions du Chapitre II portant sur les principes relatifs à la qualité des données et aux conditions de licéité des traitements.

Cette disposition concerne les traitements qui ont été régulièrement déclarés auprès de la C.C.I.N. avant la date d'entrée en vigueur de la présente loi, c'est-à-dire ceux ayant fait l'objet d'un récépissé, d'un avis ou d'une autorisation, et dont l'exploitation se poursuit.

Dès lors que ces traitements répondent aux principes de licéité prévus par la loi n° 1.165 du 23 décembre 1993, modifiée, précitée, et que leurs caractéristiques n'ont pas été modifiées, ils sont réputés avoir satisfait aux obligations dudit Chapitre.

La deuxième situation concerne les nouvelles obligations incombant aux responsables du traitement et aux sous-traitants. Pour les traitements régulièrement mis en œuvre auprès de la C.C.I.N. avant la date d'entrée en vigueur de la présente loi, et dont l'exploitation se poursuit après son entrée en vigueur, les responsables du traitement et sous-traitants disposent, à compter de cette date, d'un délai d'un an pour se mettre en conformité avec les obligations prévues aux articles 26, 27 et 28 du Chapitre IV. Ces obligations portent sur la mise en place d'un registre des activités de traitement, la désignation d'un délégué à la protection des données et la sécurité du traitement. Ce délai est porté à trois ans pour les responsables du traitement afin de procéder à l'analyse d'impact prévue à l'article 32 au titre de la réévaluation des risques.

Enfin, la troisième situation est relative à la mise en conformité des traitements avec les dispositions spécifiques des articles 66 et 67 concernant les catégories de personnes concernées et les opérations de journalisation, pour laquelle un délai de cinq ans est prévu compte tenu des contraintes techniques particulières que cette mise en conformité nécessite.

Les dispositions relatives aux droits des personnes sont d'application immédiate.

L'article 106 prévoit que l'autorité de protection informe les responsables du traitement de la nature de leurs nouvelles obligations à l'égard du traitement faisant l'objet d'une formalité lorsqu'elle est en cours d'instruction au moment de l'entrée en vigueur de la loi.

L'article 107 maintient accessible au public, pendant une durée de dix ans, la liste des traitements inscrits au répertoire institué par l'article 10 de la loi n° 1.165 du 23 décembre 1993, modifiée, précitée et mise à disposition par l'autorité de protection.

L'article 108 prévoit que les recommandations adoptées par la C.C.I.N. demeurent en vigueur jusqu'à ce qu'elles soient modifiées, remplacées ou abrogées par l'autorité de protection.

Les articles 109 à 111 actualisent les dispositions relatives aux renvois spécifiques prévus au titre de la loi n° 1.165 du 23 décembre 1993, modifiée, précitée.

L'article 112 consacre l'abandon du terme « *informations nominatives* » au profit de celui de « *données personnelles* » ou « *données à caractère personnel* » qui recouvrent, pour l'essentiel, les mêmes notions.

L'article 113 prévoit que les modalités d'application de la présente loi seront fixées par ordonnance souveraine.

L'article 114 précise que la loi se substituera, dans tous les textes législatifs et réglementaires pris avant son entrée en vigueur, à la loi n° 1.165 du 23 décembre 1993, modifiée, précitée, et consacre l'abrogation de ladite loi.

Tel est l'objet du présent projet de loi.

PROJET DE LOI

CHAPITRE I- DISPOSITIONS GENERALES

Article premier

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.

Article 2

Aux fins de la présente loi on entend par :

1. « autorité de protection » : l'autorité administrative indépendante de protection des données à caractère personnel instituée par l'article 34 ;

2. « chiffrement » : procédé de transformation cryptographique des données permettant de les rendre incompréhensibles à toute personne qui ne dispose pas de la clé de déchiffrement ;

3. « consentement de la personne concernée » : toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement ;

4. « destinataire » : la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers. Toutefois, les autorités publiques qui sont susceptibles de recevoir communication de données à caractère personnel dans le cadre d'une mission d'enquête particulière ne sont pas considérées comme des destinataires ;

5. « données à caractère personnel ou données personnelles » : toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée « personne concernée »). Est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ;

6. « données concernant la santé » : les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne ;

7. « données biométriques » : les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques ;

8. « données génétiques » : les données à caractère personnel relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé de cette personne physique et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question ;

9. « données sensibles » : les données à caractère personnel qui révèlent, directement ou indirectement, des opinions ou des appartenances politiques, raciales ou ethniques, religieuses, philosophiques ou syndicales, ou encore des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique ou des données concernant la santé, la vie sexuelle ou l'orientation sexuelle d'une personne physique ;

10. « fichier » : tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique ;

11. « groupe d'entreprises » : entreprise qui exerce le contrôle et les entreprises qu'elle contrôle du fait, par exemple, de la détention du capital, d'une participation financière ou des règles qui la régissent, ou encore du pouvoir de faire appliquer les règles relatives à la protection des données à caractère personnel ;

12. « limitation du traitement » : le marquage de données à caractère personnel conservées, en vue de limiter leur traitement futur ;

13. « organisation internationale » : une organisation internationale et les organismes de droit public international qui en relèvent, ou tout autre organisme qui est créé par un accord entre deux pays ou plus, ou en vertu d'un tel accord ;

14. « profilage » : toute forme de traitement automatisé de données à caractère personnel consistant à utiliser celles-ci pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique ;

15. « pseudonymisation » : le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable ;

16. « règles d'entreprises contraignantes » : toute règle interne relative à la protection des données à caractère personnel qu'applique un responsable du traitement ou un sous-traitant pour des transferts ou pour un ensemble de transferts de données à caractère personnel à un responsable du traitement ou à un sous-traitant établi à l'étranger au sein d'un groupe d'entreprises, ou d'un groupe d'entreprises engagées dans une activité économique conjointe ;

17. « représentant » : une personne physique ou morale établie sur le territoire de la Principauté, désignée par tous moyens écrits par le responsable du traitement ou le sous-traitant dans les conditions de l'article 24 ;

18. « responsable du traitement » : la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui détermine, seul ou conjointement avec d'autres, les finalités et les moyens du traitement ;

19. « sous-traitant » : la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement ;

20. « tiers » : une personne physique ou morale, une autorité publique, un service ou un organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont autorisées à traiter les données à caractère personnel ;

21. « traitement » : toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, notamment la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'extraction, la consultation, l'utilisation, l'adaptation ou la modification, la communication, l'archivage, l'effacement ou la destruction de données, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'application d'opérations logiques ou arithmétiques à ces données ;

22. « violation de données à caractère personnel » : une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données ;

23. « service de la société de l'information » : tout service, à titre onéreux ou non, rendu à distance et sans que les parties soient simultanément présentes, par voie électronique et à la demande individuelle d'un destinataire de services.

Article 3

1. La présente loi s'applique aux traitements de données à caractère personnel, automatisés en tout ou partie, ainsi qu'aux traitements non automatisés de données contenues ou appelées à figurer dans des fichiers :

- mis en œuvre par un responsable du traitement ou un sous-traitant établi à Monaco, que le traitement ait lieu ou non à Monaco ;

- relatifs à des personnes concernées se trouvant sur le territoire de la Principauté et mis en œuvre par un responsable du traitement ou un sous-traitant établi hors du territoire de la Principauté lorsque les activités de traitement sont liées à l'offre de biens ou de services ou au suivi du comportement de ces personnes.

2. Les dispositions de la présente loi ne sont pas applicables :

- aux traitements mis en œuvre par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques ;

- aux copies temporaires qui sont faites dans le cadre des activités techniques de transmission et de fourniture d'accès à un réseau numérique, en vue du stockage automatique, intermédiaire et transitoire des données à caractère personnel et à seule fin de permettre à d'autres destinataires du service le meilleur accès possible aux informations transmises.

CHAPITRE II – PRINCIPES RELATIFS A LA QUALITE DES DONNEES ET AUX CONDITIONS DE LICEITE DES TRAITEMENTS DE DONNEES A CARACTERE PERSONNEL

Article 4

Le responsable du traitement s'assure que les données à caractère personnel sont :

1. traitées de manière licite, loyale et transparente au regard de la personne concernée ;

2. collectées pour des finalités déterminées, explicites et légitimes, et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités. A l'exception des traitements visés aux articles 61 et 87, un traitement ultérieur de données à caractère personnel à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, est considéré comme compatible avec les finalités initiales de la collecte des données dès lors que des garanties appropriées s'appliquent ;

3. adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées ;

4. exactes et, si nécessaires, mises à jour. Le responsable du traitement prend les mesures raisonnables pour que les données à caractère personnel inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées dans les meilleurs délais ;

5. conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont traitées. Sous réserve de garanties appropriées, la durée de conservation peut être plus longue dans la mesure où les données sont traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques. Le choix des données conservées à des fins archivistiques dans l'intérêt public est opéré dans les conditions prévues par la réglementation en vigueur en matière d'archivage.

6. traitées de façon à garantir une sécurité appropriée des données à caractère personnel à l'aide de mesures techniques et organisationnelles garantissant leur intégrité et leur confidentialité.

Article 5

Pour être licite, un traitement doit répondre au moins à l'une des exigences suivantes :

1. l'obtention du consentement, pour une ou plusieurs finalités spécifiques, de la personne concernée ;

2. le besoin de respecter une obligation légale à laquelle est soumis le responsable du traitement ;

3. sa nécessité pour l'exécution d'un contrat auquel la personne concernée est partie ou l'exécution des mesures pré-contractuelles prises à la demande de celle-ci ;

4. sa nécessité pour la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique ;

5. l'existence d'un motif d'intérêt public lorsque les traitements sont mis en œuvre par une personne morale de droit public ou par une personne morale de droit privé investie d'une mission d'intérêt général ou concessionnaire d'un service public ;

6. sa nécessité pour la réalisation d'un intérêt légitime poursuivi par le responsable du traitement ou par un tiers à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant. Sont exclus de ce cas, les traitements effectués par une personne morale de droit public ou par une personne morale de droit privé investie d'une mission d'intérêt général ou concessionnaire d'un service public dans l'exécution de leurs missions.

Lorsque le traitement, mis en œuvre à une fin autre que celle pour laquelle les données ont été collectées, n'est pas fondé sur le consentement de la personne concernée ou sur une obligation légale ou réglementaire, le responsable du traitement, afin de déterminer si ledit traitement est compatible avec la finalité pour laquelle les données à caractère personnel ont été initialement collectées, tient compte, notamment :

- de l'existence éventuelle d'un lien entre les finalités pour lesquelles les données à caractère personnel ont été collectées et les finalités du traitement ultérieur envisagé ;

- du contexte dans lequel les données à caractère personnel ont été collectées, en particulier en ce qui concerne la relation entre les personnes concernées et le responsable du traitement ;

- de la nature des données à caractère personnel, en particulier si le traitement porte sur des données sensibles ou sur des données relatives aux infractions et condamnations pénales ;

- des conséquences possibles du traitement ultérieur envisagé pour les personnes concernées ;

- de l'existence de garanties appropriées pouvant comprendre le chiffrement ou la pseudonymisation.

Article 6

Lorsque le traitement est fondé sur le consentement de la personne concernée, le responsable du traitement est en mesure de démontrer que celle-ci a donné son consentement au traitement de données à caractère personnel la concernant au moyen d'un acte positif clair résultant d'une action libre, spécifique, éclairée et non équivoque. Si le consentement est donné dans le cadre d'une déclaration écrite qui concerne également d'autres questions, la demande de consentement est présentée sous une forme qui la distingue clairement de ces autres questions. Le consentement ne doit pas être exigé en contrepartie d'un bien ou d'un service à moins que le traitement faisant l'objet du consentement ne soit indispensable à la fourniture de ce bien ou service.

En présence d'une offre directe de service de la société de l'information, le consentement de la personne concernée est requis même lorsqu'elle est mineure. Toutefois, lorsque le mineur est âgé de moins de 15 ans, ce traitement n'est licite qu'en présence d'un consentement donné par le mineur concerné avec l'autorisation de la ou des personnes exerçant l'autorité parentale. Le responsable du traitement rédige en des termes clairs et simples, aisément compréhensibles par le mineur, les informations et communications relatives au traitement qui le concerne. En pareil cas, le responsable du traitement s'efforce de vérifier raisonnablement que le consentement est donné ou autorisé par le titulaire de l'autorité parentale, compte tenu des moyens technologiques disponibles.

La personne concernée ou la ou les personnes exerçant l'autorité parentale du mineur de moins de 15 ans ont le droit de retirer le consentement à tout moment. Le retrait du consentement ne compromet pas la licéité du traitement fondé sur le consentement effectué avant ce retrait. La personne concernée en est informée avant de donner son consentement. Cette dernière peut dès lors solliciter du responsable du traitement, la destruction ou l'effacement de ses données.

Sauf consentement exprès de la personne concernée, les données à caractère personnel recueillies par les prestataires de services de confiance électronique pour les besoins de la délivrance et de la conservation des certificats électroniques doivent l'être directement auprès de la personne concernée et ne peuvent être traitées que pour les fins en vue desquelles elles ont été recueillies.

Article 7

Le traitement de données sensibles est interdit.

Ne sont pas soumis à l'interdiction prévue au premier alinéa :

1. les traitements pour lesquels la personne concernée a donné son consentement explicite sauf dans le cas où la loi prévoit que cette interdiction ne peut être levée par le consentement de la personne concernée ;

2. les traitements nécessaires à la sauvegarde des intérêts vitaux de la personne concernée dans le cas où celle-ci ne peut valablement donner son consentement par suite d'une altération de ses facultés personnelles, d'une incapacité juridique ou d'une impossibilité matérielle ;

3. les traitements qui concernent les membres d'une institution ecclésiale ou d'un groupement à caractère politique, religieux, philosophique, humanitaire ou syndical, dans le cadre de l'objet statutaire ou social de l'institution ou du groupement et pour les besoins de son fonctionnement, à condition que le traitement se rapporte aux seuls membres de cet organisme ou aux personnes entretenant avec lui des contacts réguliers liés à sa finalité et que les informations ne soient pas communiquées à des tiers sans le consentement des personnes concernées ;

4. les traitements portant sur des données à caractère personnel manifestement rendues publiques par la personne concernée

5. les traitements nécessaires à la constatation, à l'exercice ou à la défense d'un droit en justice ou répondant à une obligation légale ;

6. les traitements justifiés par des motifs d'intérêt public important ;

7. les traitements nécessaires aux fins de la médecine préventive ou de la médecine du travail, de diagnostics médicaux, de l'administration de soins, de médications ou de la gestion des services de santé et de prévoyance sociale ou dans l'intérêt de la recherche ou dans le domaine de la santé publique, lorsque le traitement de ces données est effectué par un professionnel de santé soumis au secret professionnel ou par une autre personne également soumise à une obligation de secret ;

8. les traitements réalisés à des fins archivistiques dans l'intérêt public, mis en œuvre par les services ayant une obligation légale de collecte, de conservation et de communication d'archives définitives ou concernant des archives provenant d'entités privées revêtant un caractère d'intérêt public, et les traitements à des fins de recherche scientifique ou historique ou à des fins statistiques;

9. les traitements mis en œuvre par les employeurs qui portent sur des données biométriques strictement nécessaires aux contrôles de l'accès aux lieux de travail ainsi qu'aux appareils et aux applications utilisés dans le cadre des missions confiées aux employés ;

10. les traitements nécessaires à l'exécution des obligations et de l'exercice des droits propres au responsable du traitement ou à la personne concernée en matière de droit du travail, de la sécurité sociale et de la protection sociale ;

11. les traitements mis en œuvre par l'Institut Monégasque de la Statistique et des Etudes Economiques dans le cadre de ses missions ;

12. les traitements visés aux articles 61, 74 et 87 mis en œuvre par les autorités administratives et judiciaires compétentes dans le cadre des missions qui leur sont légalement conférées.

Le responsable du traitement prévoit des garanties appropriées pour la mise en œuvre des traitements visés aux chiffres 2,6, 8 à 11 afin de prévenir les risques pour les intérêts, droits et libertés fondamentales de la personne concernée, notamment un risque de discrimination

Article 8

Aucune interconnexion ne peut être effectuée entre le casier judiciaire et tout autre fichier ou traitement de données à caractère personnel mis en œuvre par une personne quelconque ou par un service ne dépendant pas de la Direction des Services Judiciaires.

CHAPITRE III - DROITS DE LA PERSONNE CONCERNEE

Article 9

Le responsable du traitement prend des mesures appropriées pour fournir toute information et procéder à toute mesure relative à l'exercice des droits de toute personne concernée, de façon concise, compréhensible et aisément accessible, en des termes clairs et simples. Les informations sont fournies gratuitement par tout moyen approprié sauf en cas de demande manifestement infondée ou abusive. Dans ce cas, le responsable du traitement peut refuser de donner suite à la demande.

Le responsable du traitement informe par écrit, dans le délai d'un mois à compter de la réception de la demande, la personne concernée des suites données à cette dernière. En cas de demande complexe ou de demandes multiples, ce délai peut être allongé de deux mois. La personne concernée en est informée de manière motivée dans le délai d'un mois à compter de la réception de sa demande. Lorsqu'il ne donne pas suite à la demande, il informe la personne concernée au plus tard dans le même délai d'un mois de la possibilité d'introduire une réclamation auprès de l'autorité de protection ou de former un recours juridictionnel de plein contentieux devant le Tribunal de Première Instance.

Lorsque le responsable du traitement a des doutes raisonnables quant à l'identité d'une personne exerçant un droit, il peut demander que lui soient fournies des informations supplémentaires nécessaires pour confirmer son identité.

Les dispositions du présent article ne sont pas applicables aux traitements visés à l'article 87.

Article 10

Lorsque les données à caractère personnel sont collectées directement auprès de la personne concernée, le responsable du traitement fournit à celle-ci, au moment où les données sont obtenues, les informations suivantes :

1. le nom et les coordonnées professionnelles du responsable du traitement et le cas échéant de son représentant à Monaco ;

2. les finalités du traitement ainsi que son fondement juridique ;

3. les intérêts légitimes poursuivis par le responsable du traitement ou par un tiers lorsque le traitement est réalisé sur le fondement du chiffre 6 de l'article 5 ;

4. les catégories de données à caractère personnel traitées ;

5. la durée de conservation des données à caractère personnel ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée ;

6. le caractère obligatoire ou facultatif des réponses ;

7. les conséquences à son égard d'un défaut de réponse ;

8. l'existence de son droit de retirer son consentement à tout moment lorsque le traitement est fondé sur l'article 5, chiffre 1, ou sur l'article 7, chiffre 1 ;

9. les destinataires ou catégories de destinataires ;

10. les moyens d'exercer son droit d'accès, d'opposition, de rectification, d'effacement, de limitation ou de portabilité relativement aux données personnelles la concernant ;

11. son droit de s'opposer à l'utilisation pour le compte de tiers, ou à la communication à des tiers de données à caractère personnel la concernant à des fins de prospection, notamment commerciale ;

12. son droit d'introduire une réclamation auprès de l'autorité de protection ;

13. le cas échéant, les coordonnées du délégué à la protection des données ;

14. le cas échéant, l'existence d'une prise de décision automatisée, y compris le profilage, et le raisonnement qui sous-tend le traitement ;

15. le cas échéant, le fait que le responsable du traitement effectue ou a l'intention d'effectuer un transfert de données à un destinataire situé hors de la Principauté et, dans l'affirmative, les dispositions mises en œuvre au titre des articles 93 à 96 ;

16. la source de provenance de ces données personnelles, lorsque celles-ci ne sont pas collectées directement auprès de la personne concernée.

Lorsque les données personnelles ne sont pas collectées auprès de la personne concernée, le responsable du traitement fournit à celle-ci, dans un délai raisonnable, les informations visées aux chiffres 1 à 16 à moins que :

- la fourniture de telles informations se révèle impossible ou exige des efforts disproportionnés ;

- l'obtention ou la communication des informations ne soit expressément prévue par la législation ou la réglementation en vigueur, en application d'engagements internationaux rendus exécutoires dans la Principauté offrant des garanties comparables ;

- le responsable du traitement soit lié par une obligation légale de secret.

Lorsque la personne concernée dispose déjà de ces informations, que les données aient été collectées directement ou non auprès d'elle, le responsable du traitement n'est pas tenu de fournir les informations prévues aux chiffres 1 à 16.

En cas de traitement ultérieur des données à caractère personnel pour une finalité autre que celle pour laquelle les données à caractère personnel ont été collectées, le responsable du traitement fournit au préalable à la personne concernée des informations au sujet de cette autre finalité et toute autre information pertinente visée au premier alinéa.

L'exercice de ce droit n'est pas applicable aux traitements visés à l'article 87.

Article 11

La personne concernée, justifiant de son identité, a le droit d'obtenir auprès du responsable du traitement, dans le délai d'un mois suivant la réception de la demande, et sous réserve de dispositions législatives spécifiques, confirmation que des données à caractère personnel la concernant sont, ou non, traitées, ainsi que les informations suivantes :

1. les finalités du traitement, les catégories de données à caractère personnel sur lesquelles il porte et les destinataires ou catégories de destinataires auxquels les données sont communiquées ;

2. lorsque cela est possible, la durée de conservation des données à caractère personnel envisagée ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée ;

3. lorsqu'elle fait l'objet d'une décision individuelle automatisée, y compris le profilage, le raisonnement qui sous-tend le traitement ;

4. toute information disponible quant à la source des données à caractère personnel non collectées auprès de la personne concernée ;

5. le droit de demander la rectification ou l'effacement de données à caractère personnel, ou une limitation du traitement des données à caractère personnel, ou le droit de s'opposer à ce traitement;

6. l'existence d'un transfert vers un pays ne bénéficiant pas de la protection adéquate ou ne présentant pas un niveau approprié de protection au regard des dispositions de la présente loi ;

7. l'existence du droit d'introduire une réclamation auprès de l'autorité de protection.

Lorsque les données personnelles sont traitées, leur communication est faite sous une forme lisible et compréhensible. Le responsable du traitement fournit une copie des données à caractère personnel faisant l'objet d'un traitement et peut exiger le paiement de frais raisonnables basés sur les coûts administratifs pour toute copie supplémentaire demandée par la personne concernée.

La communication de la copie visée à l'alinéa précédent ne doit pas porter atteinte aux droits et libertés d'autrui.

Si la personne concernée présente sa demande par voie électronique, les informations sont fournies sous une forme électronique d'usage courant, à moins que la personne concernée ne demande qu'il en soit fait autrement.

Aux fins de préserver l'intégrité du droit d'accès, le président du Tribunal de première instance ou le magistrat délégué par lui statuant en la forme des référés, peut, en cas de risque de dissimulation ou de disparition des données à caractère personnel, ordonner toutes mesures de nature à éviter cette dissimulation ou cette disparition

L'accès de la personne concernée aux informations concernant sa santé s'effectue dans les conditions prévues par la législation relative au consentement et à l'information en matière médicale.

Article 12

La personne concernée a le droit d'obtenir du responsable du traitement, sur justificatifs, la rectification, dans les meilleurs délais, de ses données personnelles si celles-ci se révèlent inexactes ou incomplètes.

Article 13

1. La personne concernée a le droit d'obtenir du responsable du traitement, dans les meilleurs délais dès qu'il en a connaissance, l'effacement, de ses données à caractère personnel dans les cas suivants :

- lorsqu'elle retire son consentement et qu'il n'existe pas d'autre fondement juridique au traitement ;

- lorsqu'elle est fondée à s'opposer au traitement en application de l'article 16 ;

- lorsque les données ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées ;

- lorsque les données ont fait l'objet d'un traitement illicite ;

- lorsque les données ont été collectées dans le cadre de l'offre de services visée au deuxième alinéa de l'article 6 ;

- pour respecter une obligation légale.

2. Les dispositions du présent article ne sont pas applicables lorsque le traitement est nécessaire :

- pour respecter une obligation légale qui requiert le traitement de ces données ;

- pour exercer une mission d'intérêt général par une personne morale de droit privé qui en est investie ou concessionnaire d'un service public ;

- pour exercer une mission relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ;

- à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, dans la mesure où l'exercice de ce droit est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs du traitement ;

- pour la constatation, l'exercice ou la défense de droits en justice ;

- pour l'exercice du droit à la liberté d'expression publique et d'information.

3. Lorsqu'il est tenu sur demande de la personne concernée de procéder à l'effacement de données personnelles qu'il a rendu publiques, le responsable du traitement en informe les autres responsables du traitement qui traitent ces données et les invite par des mesures raisonnables compte tenu des technologies disponibles et des coûts de mise en œuvre, à effacer tout lien vers ces données, toute copie et toute reproduction de ces données.

Article 14

La personne concernée a le droit d'obtenir du responsable du traitement la limitation du traitement lorsque l'un des éléments suivants s'applique :

1. l'exactitude des données à caractère personnel est contestée par la personne concernée, pendant une durée permettant au responsable du traitement de vérifier l'exactitude desdites données ;

2. le traitement est illicite et la personne concernée s'oppose à l'effacement des données et exige à la place la limitation de leur utilisation ;

3. le responsable du traitement n'a plus besoin des données à caractère personnel aux fins du traitement mais celles-ci sont encore nécessaires à la personne concernée pour la constatation, l'exercice ou la défense de droits en justice ;

4. la personne concernée s'est opposée au traitement en vertu du premier alinéa de l'article 16 pendant la vérification portant sur le point de savoir si les motifs légitimes poursuivis par le responsable du traitement prévalent sur ceux de la personne concernée.

Lorsque le traitement a été limité en vertu du premier alinéa, ces données à caractère personnel ne peuvent, à l'exception de la conservation, être traitées qu'avec le consentement de la personne concernée ou que pour la constatation, l'exercice ou la défense de droits en justice pour la protection des droits d'une autre personne physique ou morale ou encore pour des motifs importants d'intérêt public.

Le responsable du traitement tient informée la personne concernée de la limitation de ses données.

L'exercice de ce droit n'est pas applicable aux traitements visés aux articles 61, 74 et 87.

Article 15

Le responsable du traitement notifie à chaque destinataire auquel les données à caractère personnel ont été communiquées toute rectification ou tout effacement de données à caractère personnel ou toute limitation du traitement effectué conformément aux articles 12, 13, 14 ou 72, à moins qu'une telle communication se révèle impossible ou exige des efforts disproportionnés. Le responsable du traitement fournit à la personne concernée des informations sur ces destinataires si celle-ci en fait la demande.

Article 16

La personne concernée a le droit de s'opposer à tout moment, pour des raisons tenant à sa situation particulière, à un traitement fondé sur les chiffres 5 et 6 de l'article 5, sauf motif légitime justifiant la réalisation du traitement, ou pour la constatation, l'exercice ou la défense de droits en justice.

La personne concernée a le droit de s'opposer à tout moment au traitement de ses données personnelles à des fins de prospection, y compris au profilage dans la mesure où il est lié à une telle prospection.

Dans ce cas, les données à caractère personnel ne sont plus traitées à ces fins.

Dans le cadre de l'utilisation de services de la société de l'information, la personne concernée peut exercer son droit d'opposition à l'aide de procédés automatisés utilisant des spécifications techniques.

Lorsque des données à caractère personnel sont traitées à des fins de recherche scientifique ou historique ou à des fins statistiques, la personne concernée a le droit de s'opposer, pour des raisons tenant à sa situation particulière, au traitement de ses données personnelles, à moins que le traitement soit nécessaire à l'exécution d'une mission d'intérêt général par une personne morale de droit privé qui en est investie ou concessionnaire d'un service public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement.

L'exercice de ce droit n'est pas applicable aux traitements visés aux articles 61, 74 et 87.

Par exception à l'article 10, le responsable du traitement informe clairement la personne concernée de son droit d'opposition au plus tard au moment de la première communication de manière séparée de toute autre information.

Article 17

La personne concernée a le droit de recevoir ses données personnelles qu'elle a fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et a le droit de transmettre ces données à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle, lorsque les conditions suivantes sont remplies :

- la personne concernée a consenti au traitement de ses données à caractère personnel ou lorsque le traitement est prévu par un contrat, tel que visé au chiffre 3 de l'article 5 ;

- le traitement est effectué à l'aide de procédés automatisés.

Lorsque la personne concernée exerce son droit à la portabilité des données en application des dispositions du premier alinéa, elle a le droit d'obtenir que ses données personnelles soient transmises directement d'un responsable du traitement à un autre, lorsque cela est techniquement possible.

Le droit visé au premier alinéa s'exerce sans préjudice de l'article 13. Il ne s'applique pas au traitement nécessaire à l'exécution d'une mission d'intérêt général par une personne morale de droit privé qui en est investie ou concessionnaire d'un service public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement.

Le droit mentionné au premier alinéa ne doit pas porter atteinte aux droits et libertés des tiers.

Article 18

Toute personne a le droit de ne pas être soumise à une décision produisant des effets juridiques à son égard ou l'affectant de manière significative, prise sur le seul fondement d'un traitement automatisé, y compris le profilage.

Une personne peut toutefois être soumise à une décision mentionnée au précédent alinéa lorsque cette décision est soit :

1. prise dans le cadre de la conclusion ou de l'exécution d'un contrat entre la personne concernée et un responsable du traitement, à condition que la demande de conclusion ou d'exécution du contrat, introduite par la personne concernée, ait été satisfaite ou que des mesures appropriées, telles que la possibilité de faire valoir son point de vue et de voir réexaminer sa demande, garantissent la sauvegarde de son intérêt légitime ;

2. autorisée par des dispositions législatives ou réglementaires qui précisent les mesures garantissant la sauvegarde des droits et libertés et de l'intérêt légitime de la personne concernée ;

3. fondée sur le consentement explicite de la personne concernée, à condition que des garanties appropriées sauvegardant les intérêts légitimes de celle-ci aient été prises par le responsable du traitement, au moins le droit d'obtenir du responsable du traitement une intervention humaine, de faire valoir son point de vue et de voir réexaminer sa demande, garantissent la sauvegarde de son intérêt légitime ;

4. en présence de données sensibles, fondée sur le consentement explicite de la personne concernée ou justifiée par des motifs d'intérêt public, à condition que des garanties appropriées, de même nature que celles prévues au chiffre 3 ci-dessus, aient été prises par le responsable du traitement.

Article 19

Sauf dispositions législatives contraires, l'ascendant, le descendant jusqu'au second degré, le conjoint survivant d'une personne décédée ou le cohabitant ou le partenaire au sens de la loi n° 1.481 du 17 décembre 2019, peut, s'il justifie d'un intérêt, exercer les droits prévus aux articles 11, 12, 13, 14, 16 et 17 pour ce qui est des informations concernant cette personne.

Article 20

Dans l'exercice des missions qui leur sont légalement conférées, le responsable du traitement ou le sous-traitant peuvent, sous réserve d'y être habilités et à la condition que cela respecte l'essence des droits et liberté fondamentaux et constitue une mesure nécessaire et proportionnée, faire exception à l'article 4 ainsi qu'aux droits et obligations énumérés aux articles 9 à 18 et 29 afin de garantir :

1. la sécurité nationale ;

2. la sécurité publique ;

3. la prévention et la détection des infractions pénales, ainsi que les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique ou la prévention de telles menaces ;

4. l'indépendance de la justice et des procédures judiciaires ;

5. les intérêts économiques et financiers, notamment dans les domaines monétaire, budgétaire et fiscal, la santé publique ou la sécurité sociale ;

6. une mission de contrôle, d'inspection et de réglementation liée à l'exercice de l'autorité publique dans le cadre des traitements visés aux chiffres 1 et 5 ;

7. la prévention et la détection de manquements à la déontologie des professions réglementées, ainsi que les enquêtes et les poursuites en la matière ;

8. la liberté d'expression publique ;

9. l'exécution en matière civile, des décisions ou actes au sens de l'article 470 du Code de procédure civile et des titres de créance au sens des articles 490 et 495 du même Code.

Les dispositions spécifiques relatives aux finalités du traitement ou des catégories de traitement, aux catégories de données à caractère personnel, à l'étendue des limitations, aux garanties destinées à prévenir les abus ou l'accès ou le transfert illicite, à la détermination du responsable du traitement ou des catégories de responsables du traitement, aux durées de conservation et aux garanties applicables, aux risques pour les droits et libertés des personnes concernées et au droit des personnes concernées d'être informées de la limitation, sont en tant que de besoin précisées dans l'acte juridique qui crée le traitement.

CHAPITRE IV - OBLIGATIONS INCOMBANT AU RESPONSABLE DU TRAITEMENT ET AU SOUS-TRAITANT

Section I - Obligations générales

Article 21

Au regard de la nature, de la portée, du contexte et des finalités du traitement, le responsable du traitement s'assure que le traitement est effectué conformément aux dispositions de la présente loi et est en mesure de le démontrer.

Le responsable du traitement et le sous-traitant ainsi que, le cas échéant, leurs représentants coopèrent avec l'autorité de protection, à la demande de celle-ci, dans l'exécution de ses missions.

L'application d'un code de conduite validé dans les conditions de l'article 30 ou de mécanismes de certification approuvés dans les conditions de l'article 31 peut servir d'élément pour démontrer le respect des obligations incombant au responsable du traitement.

Article 22

Au regard des risques présentés par le traitement et de la nature des données personnelles, le responsable du traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées afin de protéger les droits de la personne concernée.

Lesdites mesures consistent à :

- assurer dès la conception la conformité du traitement aux principes relatifs à la protection des données de façon effective ;

- assortir le traitement des garanties nécessaires afin de répondre aux exigences de la présente loi.

Le responsable du traitement met également en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées. Cela s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité. En particulier, ces mesures garantissent que, par défaut, les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques sans l'intervention de la personne concernée.

Article 23

Si deux responsables du traitement ou plus déterminent ensemble les finalités et les moyens du traitement, ils sont considérés comme étant les responsables conjoints du traitement.

De ce fait, ils définissent de manière transparente au sein d'un accord leurs obligations respectives, notamment en ce qui concerne l'exercice des droits de la personne concernée et la communication des informations visées à l'article 10.

Indépendamment des termes de l'accord visé à l'alinéa précédent, la personne concernée peut exercer les droits que lui confère la présente loi à l'égard de l'un ou de l'autre, et contre chacun des responsables de traitement.

Article 24

Lorsque le traitement concerne le second tiret du chiffre 1 de l'article 3, le responsable du traitement ou le sous-traitant désigne par tous moyens écrits un représentant dans la Principauté. Ce dernier est mandaté pour être le contact des personnes concernées par le traitement et de l'autorité de protection à qui elles peuvent s'adresser pour toutes questions.

Cette obligation ne s'applique pas :

- à un traitement occasionnel, qui n'implique pas un traitement à grande échelle de données sensibles ;

- à un traitement de données à caractère personnel relatives à des condamnations pénales ou à des infractions mis en œuvre au titre des articles 61, 77 et 87 ;

- si le responsable du traitement est une personne morale de droit public ou un organisme public.

La désignation d'un représentant est sans préjudice d'actions en justice qui pourraient être intentées contre le responsable du traitement ou le sous-traitant.

Article 25

Lorsque le responsable du traitement a recours aux services d'un sous-traitant, celui-ci doit présenter les garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à assurer la protection des données personnelles et le respect des droits des personnes concernées.

La réalisation de traitements par un sous-traitant est régie par un contrat définissant l'objet et la durée du traitement, la nature et la ou les finalités du traitement, le type de données à caractère personnel et les catégories de personnes concernées ainsi que les obligations et les droits du responsable du traitement. Ce contrat prévoit notamment, que le sous-traitant :

1. ne traite les données à caractère personnel que sur instruction documentée du responsable du traitement ;

2. veille au respect de la confidentialité ;

3. prend toutes les mesures requises en matière de sécurité des données à caractère personnel ;

4. selon le choix du responsable du traitement, supprime toutes les données à caractère personnel ou les renvoie au responsable du traitement au terme de la prestation de services relatifs au traitement, et détruit les copies existantes ;

5. met à la disposition du responsable du traitement toutes les informations nécessaires pour démontrer le respect de ses obligations ;

6. apporte son concours au responsable du traitement pour garantir le respect des obligations prévues aux articles 28, 29, 32 et 33.

Le sous-traitant informe immédiatement le responsable du traitement si, selon lui, une instruction constitue une violation de la présente loi.

Le sous-traitant ne peut lui-même sous-traiter un traitement à un tiers qu'avec l'autorisation écrite préalable du responsable du traitement et dans le respect des dispositions énoncées au présent article.

Le sous-traitant est considéré comme responsable du traitement, si en violation de la présente loi, il détermine les finalités et les moyens du traitement.

L'application, par un sous-traitant, d'un code de conduite validé dans les conditions de l'article 30 ou de mécanismes de certification approuvés dans les conditions de l'article 31 peut servir d'élément pour démontrer l'existence des garanties suffisantes prévues au premier alinéa du présent article.

Article 26

1. Le responsable du traitement, ou le cas échéant son représentant, tient un registre des activités de traitement effectuées sous sa responsabilité.

Ce registre contient au moins les indications suivantes :

- le nom et les coordonnées du responsable du traitement et, le cas échéant, du responsable conjoint, du représentant du responsable du traitement et du délégué à la protection des données ;

- les finalités du traitement ;

- les catégories de personnes concernées et les catégories de données à caractère personnel traitées ;

- les catégories de destinataires ;

- dans la mesure du possible, le délai de conservation des données à caractère personnel ou les critères pour déterminer la durée de conservation ;

- dans la mesure du possible, une description générale des mesures visant à garantir la sécurité des données visées à l'article 28 ;

- en cas de transfert de données à caractère personnel hors de la Principauté l'identification du pays destinataire ou de l'organisation internationale et, le cas échéant, les garanties prévues à l'article 94 ;

- le cas échéant, le recours au profilage pour les traitements visés à l'article 61 ;

- une indication de la base juridique de l'opération de traitement, y compris les transferts, pour les traitements visés aux articles 61 et 87.

2. Le sous-traitant tient un registre de toutes les catégories d'activités de traitement effectuées pour le compte du ou des responsables du traitement.

Ce registre contient au moins les indications suivantes :

- le nom et les coordonnées du sous-traitant et de chaque responsable du traitement pour le compte duquel le sous-traitant agit, et, le cas échéant, le nom et les coordonnées du représentant du responsable du traitement ou du sous-traitant et du délégué à la protection des données ;

- les catégories de traitements effectuées pour le compte de chaque responsable du traitement ;

- dans la mesure du possible, une description générale des mesures visant à garantir la sécurité des données visées à l'article 28 ;

- en cas de transfert de données à caractère personnel hors de la Principauté ou à une organisation internationale, l'identification du pays destinataire ou de l'organisation internationale et, le cas échéant, les garanties prévues à l'article 93.

3. Le responsable du traitement ou le sous-traitant et, le cas échéant, leurs représentants mettent leur registre à la disposition de l'autorité de protection sur simple demande.

4. Les obligations visées aux précédents alinéas ne s'appliquent pas aux entreprises ou organisations établies en Principauté comptant moins de 50 salariés sauf si le traitement est susceptible de comporter un risque pour les droits et libertés des personnes concernées ou s'il n'est pas occasionnel ou s'il porte sur des données sensibles ou sur des données personnelles relatives à des infractions, des condamnations pénales et mesures de sûreté ou portant sur des soupçons d'activités illicites.

Article 27

Le responsable du traitement et le sous-traitant peuvent désigner un délégué à la protection des données chargé :

- d'informer et conseiller le responsable du traitement ou le sous-traitant ainsi que les employés qui procèdent au traitement sur les obligations qui leur incombent en vertu de la présente loi ;

- de contrôler le respect de la présente loi en matière de protection des données personnelles ainsi que des règles internes du responsable du traitement ou du sous-traitant en matière de protection des données personnelles ;

- de dispenser des conseils, sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données personnelles ;

- de coopérer avec l'autorité de protection et d'être son correspondant sur les questions relatives au traitement ;

- de présenter à l'autorité de protection les demandes d'avis lorsqu'elles portent sur un traitement visé aux articles 61 et 74.

Le délégué à la protection des données tient compte du risque associé aux opérations de traitement compte tenu de la nature, de la portée, du contexte et des finalités du traitement.

Le responsable du traitement et le sous-traitant veillent à ce que le délégué à la protection des données soit associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel.

A l'exception des juridictions dans l'exercice de leurs fonctions juridictionnelles, la désignation du délégué à la protection des données visé au précédent alinéa est obligatoire lorsque :

- le traitement est effectué par une personne morale de droit public ou une personne morale de droit privé investie d'une mission d'intérêt général ou concessionnaire d'un service public ;

- les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées ;

- les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de données sensibles ou de données à caractère personnel relatives à des condamnations pénales ou à des infractions.

Un seul délégué à la protection des données peut être désigné pour plusieurs personnes morales de droit public ou pour plusieurs personnes morales de droit privé investies d'une mission d'intérêt général ou concessionnaires d'un service public.

Un groupe d'entreprises peut désigner un seul délégué à la protection des données à condition qu'il soit facilement joignable à partir de chaque lieu d'établissement.

Le responsable du traitement et le sous-traitant fournissent au délégué à la protection des données les moyens nécessaires pour exercer sa mission, ainsi que l'accès aux données et aux opérations de traitement, à l'exception des traitements visés aux articles 61 et 87. Dans ce cadre, ce dernier agit en toute indépendance et ne reçoit d'instructions d'aucune autorité.

Le délégué à la protection des données ne peut être relevé de ses fonctions ou pénalisé par le responsable du traitement ou le sous-traitant pour l'exercice de ses missions.

Le délégué à la protection des données est soumis à une obligation de confidentialité en ce qui concerne l'exercice de ses missions.

Le responsable du traitement ou le sous-traitant publient les coordonnées professionnelles du délégué à la protection des données et les communiquent à l'autorité de protection.

Section II - Obligations spécifiques

Article 28

Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement, le responsable du traitement et le sous-traitant prennent des mesures techniques et organisationnelles appropriées, afin de garantir un niveau de sécurité adapté aux risques pour les droits et libertés des personnes physiques, notamment la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel ou l'accès non autorisé à de telles données, de manière accidentelle ou illicite.

A cette fin, le responsable du traitement et le sous-traitant prennent des mesures telles que la pseudonymisation et le chiffrement des données, ou tout moyen permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement de même que tout moyen permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique, ou encore la mise en place d'une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

Lorsque le responsable du traitement ou le sous-traitant a recours aux services d'un ou plusieurs prestataires, il s'assure que ces derniers sont en mesure de satisfaire aux obligations visées aux précédents alinéas.

La mise en œuvre d'un code de conduite tel que décrit à l'article 30 ou d'un mécanisme de certification tel que prévu à l'article 31 participe à la démonstration, par le responsable du traitement ou le sous-traitant, du respect de ses obligations en matière de sécurité.

Les dispositions prévues au précédent alinéa ne sont pas applicables aux traitements visés aux articles 61, 74 et 87.

Article 29

Le responsable du traitement notifie à l'autorité de protection sans délai excessif, et si possible dans un délai maximum de soixante-douze heures, les violations de données à caractère personnel dont il a connaissance à moins que la violation ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes concernées.

La notification visée au premier alinéa précise :

1. la nature de la violation y compris, dans la mesure du possible, les catégories et le nombre approximatif de personnes concernées par la violation ;

2. le nom et les coordonnées du délégué à la protection des données lorsque celui-ci a été désigné ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;

3. les conséquences probables de la violation ;

4. les mesures prises ou celles qu'il propose de prendre pour remédier à la violation.

Le responsable du traitement documente toute violation de données à caractère personnel en indiquant les faits concernant la violation, ses effets et les mesures prises pour y remédier.

Le sous-traitant notifie au responsable du traitement toute violation de données à caractère personnel dès qu'il en a connaissance.

Lorsque la violation de données est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement communique ladite violation à la personne concernée dans les meilleurs délais. Cette communication décrit en termes clairs la nature de la violation, et contient les informations et mesures visées aux chiffres 2, 3 et 4.

La communication visée à l'alinéa précédent n'est pas nécessaire si l'une des conditions ci-après est remplie :

- les données affectées par la violation ont préalablement fait l'objet de mesures de protection technique et organisationnelle qui rendent lesdites données incompréhensibles pour toute personne n'étant pas autorisée à y accéder ;

- le devoir d'informer individuellement la personne concernée nécessiterait des efforts disproportionnés ;

- les mesures ultérieures prises par le responsable du traitement garantissent que le risque n'est plus susceptible de se matérialiser.

L'autorité de protection peut exiger du responsable du traitement qu'il procède à la communication de la violation à la personne concernée si cela n'a pas été fait.

Article 30

Les associations et organismes professionnels représentant des catégories de responsables du traitement ou de sous-traitants peuvent élaborer des codes de conduite destinés à contribuer à la bonne application de la présente loi.

Les codes de conduite de même que leurs modifications ultérieures ou, le cas échéant, les prorogations de codes existants sont transmis à l'autorité de protection qui vérifie qu'ils offrent les garanties de protection appropriées.

Lorsque le code de conduite a déjà été approuvé par une autorité de protection étrangère, le responsable du traitement ou le sous-traitant transmet ledit code à l'autorité de protection qui en vérifie les dispositions au regard de la présente loi.

L'autorité de protection valide et publie les codes de conduite applicables à Monaco.

L'application des codes de conduite approuvés et publiés revêt un caractère obligatoire pour leurs adhérents.

Les codes de conduite, leurs modifications et, le cas échéant, leurs prorogations sont répertoriés par l'autorité de protection dans un registre accessible au public.

Les dispositions du présent article ne sont pas applicables aux traitements visés aux articles 61, 74 et 87.

Article 31

Une procédure de certification est instituée en matière de protection des données à caractère personnel. Elle peut être mise en œuvre par l'autorité de protection ou par des organismes indépendants agréés par ladite autorité.

L'organisme demandant l'agrément doit justifier d'une expertise au regard de l'objet de la certification et répondre à des critères pris par arrêté ministériel sur proposition de l'autorité de protection.

Au regard des garanties apportées, ladite autorité agrée l'organisme demandeur pour une durée de cinq ans renouvelable.

L'organisme de certification ainsi agréé est habilité à délivrer une certification attestant que le responsable du traitement ou le sous-traitant respecte les dispositions de la présente loi et des textes règlementaires pris pour son application.

La certification délivrée par un organisme agréé d'un Etat membre de l'Union européenne ou justifiant d'un niveau de protection adéquat peut être reconnue par l'autorité de protection.

Les dispositions du présent article ne sont pas applicables aux traitements visés aux articles 61, 74 et 87.

Article 32

Lorsque le traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et de ses finalités, est susceptible d'entraîner un risque élevé pour les droits et libertés des personnes concernées, le responsable du traitement effectue préalablement au traitement, et après avoir pris conseil auprès du délégué à la protection des données lorsque celui-ci a été désigné, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel. Une seule et même analyse d'impact peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires.

Un risque élevé existe notamment dans les cas suivants :

a) l'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative ;

b) le traitement à grande échelle de données sensibles ou de données à caractère personnel relatives aux infractions, condamnations pénales et mesures de sureté ou portant sur des soupçons d'activité illicites ;

c) la surveillance systématique à grande échelle de zone accessible au public ;

d) l'utilisation à grande échelle d'un identifiant numérique.

Cette analyse d'impact contient au moins :

- une description générale des opérations de traitement envisagées et des finalités du traitement, y compris, le cas échéant, l'intérêt légitime poursuivi par le responsable du traitement ;

- une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités ;

- une évaluation des risques pour les droits et libertés des personnes concernées conformément au paragraphe 1 ;

- les mesures envisagées pour faire face aux risques.

Un arrêté ministériel établit la liste des critères permettant de déterminer si un traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques.

L'analyse d'impact est conservée à titre probatoire par le responsable du traitement et communiquée sur demande à l'autorité de protection.

Le responsable du traitement procède à une réévaluation de l'analyse d'impact en cas de modification du risque.

Les dispositions du présent article ne sont pas applicables aux traitements soumis aux formalités préalables prévues aux articles 55 et 88.

Article 33

Le responsable du traitement consulte l'autorité de protection préalablement à la mise en œuvre du traitement lorsque l'analyse d'impact effectuée au titre de l'article 32 indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque.

Le responsable du traitement communique alors à l'autorité de protection :

1. les responsabilités respectives du responsable du traitement, des responsables conjoints et des sous-traitants participant au traitement et les coordonnées du délégué à la protection des données lorsque celui-ci a été désigné ;

2. les finalités et les moyens du traitement envisagé ;

3. les mesures et les garanties prévues afin de protéger les droits et libertés des personnes concernées ;

4. l'analyse d'impact relative à la protection des données prévue à l'article 32 ;

5. toute autre information demandée par l'autorité de protection.

L'autorité de protection fournit dans un délai maximum de huit semaines un avis écrit au responsable du traitement. Le délai peut être prolongé de six semaines lorsqu'il s'agit d'un traitement complexe. Si l'autorité de protection considère que le traitement constituerait en l'état une violation, elle impose au responsable du traitement de prendre les mesures appropriées et peut faire usage des pouvoirs prévus à l'article 43.

CHAPITRE V - DE L'AUTORITE DE PROTECTION DES DONNEES PERSONNELLES

Section I - Fonctionnement

Article 34

Il est créé une autorité administrative indépendante dénommée Autorité de Protection des Données Personnelles (A.P.D.P.).

L'autorité de protection se réunit en formation plénière ou en formation restreinte telle que définie à l'article 38.

Elle est chargée de contrôler et vérifier que les données personnelles sont traitées en conformité avec les dispositions législatives et réglementaires en vigueur en matière de protection des données à caractère personnel.

Sont exclus de la compétence de l'autorité :

1. les traitements effectués par les juridictions et le ministère public dans l'exercice de leurs fonctions juridictionnelles ainsi que ceux effectués dans le cadre des procédures d'entraide judiciaire internationale, dont le contrôle relève d'un Délégué judiciaire à la protection des données désigné par arrêté directorial du Secrétaire d'Etat à la Justice, Directeur des Services Judiciaires ;

2. les traitements intéressant la sûreté de l'État et la sécurité nationale régis par les dispositions des articles 9 à 15 et 18 de la loi n° 1.430 du 13 juillet 2016 portant diverses mesures relatives à la préservation de la sécurité nationale qui relèvent de l'autorité de contrôle spécifique formée par la Commission instituée par l'article 16 de ladite loi, sont contrôlés au regard de la règlementation en vigueur en matière de données personnelles conformément aux dispositions de la section VI du Chapitre VII de la présente loi.

Article 35

L'autorité de protection a pour missions :

1. de favoriser la sensibilisation du public à ses fonctions, à ses pouvoirs et à ses activités ainsi que sa compréhension des risques, des règles, des garanties et des droits relatifs à la protection des données personnelles et de l'attention particulière portée au droit à la protection des données des enfants et des personnes vulnérables ;

2. d'informer les personnes concernées des droits et obligations issus de la présente loi, notamment par la communication sur demande à toute personne, ou par la publication, si l'autorité de protection l'estime utile à l'information du public, de ses délibérations, avis ou recommandations de portée générale, sauf lorsqu'une telle communication ou publication serait de nature à porter atteinte à la sécurité publique ou au respect dû à la vie privée et familiale ;

3. de conseiller les responsables du traitement et les sous-traitants en ce qui concerne les obligations qui leur incombent en vertu de la présente loi ;

4. d'émettre un avis motivé sur les traitements visés à l'article 55 ;

5. de tenir à la disposition du public la liste des traitements visés à l'article 55 ;

6. d'émettre un avis motivé sur les analyses d'impact présentant un risque élevé conformément aux dispositions de l'article 33 ;

7. d'autoriser le transfert de données à caractère personnel conformément aux dispositions de l'article 96 ;

8. de procéder à des vérifications et des investigations conformément à l'article 43 et de notifier au responsable du traitement ou au sous-traitant les manquements constatés à la présente loi ;

9. de tenir des registres internes des violations de la loi et des mesures correctrices prises par ses soins ;

10. de dénoncer au procureur général les faits constitutifs d'infractions dont elle a connaissance dans l'exercice de ses missions ;

11. d'instruire toutes réclamations formulées par les personnes concernées sur le fondement de la présente loi et de les informer des suites données ;

12. d'assurer la mise en œuvre du droit d'accès indirect, dans les conditions prévues à l'article 71 ;

13. de valider et publier les codes de conduite visés à l'article 30 ;

14. de délivrer des certifications et des agréments aux organismes de certification dans les conditions visées à l'article 31 et de procéder à l'examen périodique des certifications délivrées ;

15. d'adopter et de publier des lignes directrices ou des recommandations destinées à faciliter l'application des règles prévues par la présente loi, notamment au titre des articles 30, 31 et 32 ;

16. d'approuver et de publier les clauses contractuelles types établies conformément aux règles de l'art et les règles d'entreprises contraignantes visées à l'article 94 ;

17. d'alerter le Ministre d'Etat de l'évolution des pratiques, des législations et des règlementations qui ne permettrait plus à un Etat d'être reconnu comme disposant d'un niveau d'un niveau de protection adéquat par la Principauté ;

18. de publier la liste des pays disposant d'un niveau de protection adéquat au sens de l'article 93 ;

19. de coopérer avec les autorités de protection étrangères conformément aux dispositions de l'article 42 ;

20. d'établir un rapport annuel d'activité remis au Ministre d'État, au Secrétaire d'État à la Justice, Directeur des Services Judiciaires et au Président du Conseil National. Ce rapport est public.

L'autorité de protection est consultée par le Ministre d'État ou par le Secrétaire d'État à la Justice, Directeur des Services Judiciaires, lors de l'élaboration de mesures législatives, réglementaires ou d'arrêtés directoriaux pris au titre de l'administration de la justice ayant pour objet la protection des données à caractère personnel ou au traitement de telles données et peut l'être également sur toutes mesures ayant trait à la protection des données.

L'autorité de protection peut être consultée par le Président du Conseil National lors de l'élaboration de propositions de loi relatives à la protection des données à caractère personnel ou au traitement de telles données.

Lorsqu'elle est consultée dans le cadre des deux précédents alinéas, elle rend son avis dans un délai de deux mois, renouvelable une fois sur décision motivée de son président.

En cas d'urgence avérée et motivée, ce délai peut être réduit à la demande du Ministre d'État ou du Secrétaire d'État à la Justice, Directeur des Services Judiciaires, sans qu'il puisse être inférieur à un mois, sauf circonstances exceptionnelles justifiées qui exigeraient une durée plus courte.

L'autorité de protection peut également proposer au Ministre d'État l'instauration de dispositions particulières dans le domaine de la protection des données, notamment à l'égard de l'utilisation des nouvelles technologies.

Les avis de l'autorité de protection peuvent être rendus publics par l'autorité qui les a sollicités ou, avec l'accord de celle-ci, par l'autorité de protection.

Article 36

Sans préjudice de tout recours juridictionnel, la personne concernée dont les droits conférés par la présente loi ou les textes pris pour son application ont été méconnus, ou celle ayant des raisons de présumer que ces droits ont été méconnus, peut saisir le président de l'autorité de protection, aux fins, le cas échéant, de mise en œuvre des mesures prévues à la section II.

L'autorité de protection informe la personne concernée auteur de la saisine de l'état d'avancement et de l'issue de sa réclamation.

Cette information mentionne le droit de la personne concernée d'introduire un recours juridictionnel effectif auprès du Tribunal de première instance, en cas d'absence de réponse à l'issue d'un délai de trois mois à compter de la notification de la saisine.

Les réclamations portant sur les traitements mis en œuvre par les juridictions dans l'exercice de leurs fonctions juridictionnelles et par le ministère public relèvent de la juridiction concernée par la procédure au cours de laquelle les données ont été collectées.

Article 37

Les membres de l'autorité de protection sont nommés par ordonnance souveraine pour un mandat de cinq ans renouvelable une fois.

L'autorité de protection est composée de huit membres titulaires proposés, en raison de leur compétence comme suit :

1. un membre par le Ministre d'État ;
2. un membre par le Conseil National ;
3. un membre par le Conseil d'État ;
4. un membre ayant qualité de magistrat du siège par le premier Président de la Cour d'Appel, président de la formation restreinte ;
5. un membre par le Conseil Communal ;
6. un membre par le Conseil Économique, Social et Environnemental ;
7. un membre ayant qualité de magistrat en activité ou en retraite ayant exercé dans une juridiction monégasque par le premier Président de la Cour de Révision ;
8. un membre qualifié dans le domaine de la santé par le Comité de la Santé Publique.

Compte tenu des fonctions qui lui sont dévolues par l'article 43, le membre ayant qualité de magistrat en activité ou en retraite proposé par le premier Président de la Cour de Révision ne peut siéger dans la formation restreinte prévue à l'article 38.

Les propositions concernant les membres visés aux chiffres 1, 2, 3, 5, 6 et 8 sont faites hors des autorités, conseils et institutions concernés selon des modalités fixées par ordonnance souveraine.

L'autorité de protection élit en son sein, à la majorité absolue, un président et un vice-président, lesquels ne peuvent siéger dans la formation restreinte prévue à l'article 38.

Lorsqu'au cours de son mandat, un membre cesse ou n'est plus en mesure d'exercer ses fonctions, le président en informe l'autorité proposante concernée en vue de la nomination d'un nouveau titulaire pour la période courant jusqu'à l'expiration dudit mandat.

Sauf démission ou empêchement, il ne peut être mis fin aux fonctions d'un membre de l'autorité de protection sauf en cas d'agissement grave constitutif d'un manquement fautif aux devoirs de bonne moralité et de probité et aux règles de déontologie auxquels il est tenu.

Dans l'exercice de leurs attributions, les membres de l'autorité de protection ne reçoivent d'instruction d'aucune autorité.

La voix du président est prépondérante en cas de partage égal des voix.

Article 38

La formation restreinte instituée par l'article 34 est chargée de prendre les mesures et de prononcer les sanctions prévues à l'article 48 à l'encontre des responsables du traitement ou des sous-traitants qui ne respectent pas les dispositions de la présente loi.

Cette formation est composée du magistrat du siège, mentionné à l'article 37, président et de deux autres membres élus par l'autorité en son sein.

Ses membres ne peuvent exercer aucune attribution en matière d'instruction et de poursuites.

La formation restreinte délibère hors la présence du personnel des services de l'autorité de protection, à l'exception d'un secrétaire de séance.

Article 39

Les membres de l'autorité de protection s'abstiennent de tout acte incompatible avec leur mandat.

La qualité de membre de l'autorité de protection est incompatible avec :

- celle de conseiller national ou communal ;

- celle de conseiller d'État ;

- celle de magistrat en position d'activité, sauf pour les membres visés aux chiffres 4 et 7 de l'article 37 ;

- celle de fonctionnaire ou d'agent de l'État, de la Commune ou d'un établissement public, en position d'activité ;

- l'exercice de fonctions ou la détention de participations dans des entreprises monégasques ou étrangères concourant à la fabrication de matériel utilisé en informatique ou en communications électroniques ou à la fourniture de services en informatique ou en communications électroniques ou concourant au commerce de biens matériels et immatériels ou de prestations de service dans ces domaines.

Article 40

Les membres de l'autorité de protection, le personnel de ses services ainsi que toute personne dont elle s'assure le concours, sont tenus pour tout ce qui concerne les faits et informations dont ils ont connaissance dans l'exercice de leurs fonctions, au secret professionnel sous les sanctions prévues à l'article 308 du code pénal et sous peine de se voir relever de leurs fonctions par application de l'article 37.

Ils sont également tenus, sous peine de poursuites, à une obligation de discrétion y compris après la fin de leur mandat ou de leurs fonctions par rapport aux éléments qu'ils ont eu à connaitre en raison de leur mandat ou de leurs fonctions.

Article 41

L'autorité de protection dispose d'un budget propre inscrit dans un Chapitre spécifique du budget de l'État.

Les dépenses sont ordonnancées par le président de l'autorité de protection ou le secrétaire général. Les comptes de l'autorité de protection sont vérifiés annuellement dans les conditions fixées par ordonnance souveraine.

Le président de l'autorité de protection représente ladite autorité et conclut à ce titre tous contrats nécessaires au bon fonctionnement de ses services.

En cas d'absence ou d'empêchement du président, son remplacement est assuré par le vice-président.

Les services de l'autorité de protection sont dirigés par le président. Ils comprennent le secrétaire général et les agents du secrétariat. Le secrétaire général est chargé du fonctionnement et de la coordination des services.

Le personnel de ses services peut être composé de fonctionnaires, placés en position de détachement auprès de l'autorité de protection en application des dispositions législatives et réglementaires en vigueur en la matière.

Les autres membres du personnel sont choisis et recrutés par le président sur le fondement d'un contrat établi selon les formes et règles générales applicables aux agents de l'État.

Sauf dispositions législatives ou réglementaires spécifiques, le personnel des services de l'autorité de protection est soumis aux règles générales applicables aux fonctionnaires et agents de l'État.

Toutefois, les pouvoirs hiérarchiques et disciplinaires sont exercés à son endroit par le président de l'autorité de protection.

L'autorité de protection établit et publie sur son site internet son règlement intérieur.

Le président de l'autorité de protection est chargé de représenter l'État en justice à raisons des activités et du fonctionnement de ladite autorité.

Article 42

1. L'autorité de protection coopère avec les autorités étrangères chargées de la protection des données offrant un niveau de garantie équivalent ou approprié. A ce titre, elle prête assistance pour l'accomplissement de leurs missions en :

- échangeant des informations pertinentes ou des données à caractère personnel faisant l'objet d'un traitement à la condition que ces données soient essentielles à la coopération ou que la personne concernée ait préalablement donné son consentement ;

- fournissant des informations sur ses pratiques en matière de protection des données à caractère personnel ;

- en coordonnant ses vérifications ou investigations ou en menant des actions conjointes.

2. Pour faire droit à la demande d'assistance, celle-ci doit notamment contenir la finalité et les motifs de la demande, ainsi que toutes informations utiles.

3. Lorsqu'elle est sollicitée par une autorité de contrôle étrangère et qu'elle entend donner suite à la demande, l'autorité de protection prend toute mesure appropriée pour répondre à cette demande dans les meilleurs délais à compter de sa réception. Elle informe l'autorité étrangère des résultats obtenus ou, selon le cas, des mesures envisagées ou prises pour donner suite à la demande.

Elle ne perçoit pas de frais pour les actions qu'elle entreprend à la suite d'une demande d'assistance mutuelle. Toutefois, dans des circonstances exceptionnelles, elle peut convenir avec l'autorité de contrôle demanderesse de règles de dédommagements pour des dépenses spécifiques liées à la demande d'assistance mutuelle.

4. L'autorité de protection refuse de donner suite à une demande de coopération si :

- la demande est incompatible avec ses compétences ;

- la demande n'est pas conforme aux dispositions de la présente loi ;

- l'exécution de la demande est incompatible avec la souveraineté, la sécurité nationale, l'ordre public ou le droit monégasque ;

- la réciprocité n'est pas garantie ;

- les données personnelles échangées ne sont pas utilisées exclusivement aux fins pour lesquelles elles ont été demandées ;

- l'autorité étrangère de protection ne s'est pas engagée à ne pas divulguer les informations ou données communiquées à des tiers sans son accord préalable.

Dans ces cas, l'autorité de protection communique à l'autorité de contrôle étrangère les motifs de son refus d'assistance.

Section II - Du contrôle de la mise en œuvre des traitements

Article 43

1. L'autorité de protection, hors formation restreinte, fait procéder d'office ou sur signalement aux vérifications et investigations, nécessaires au contrôle de la mise en œuvre des traitements, par des membres de l'autorité de protection ou par des agents de son secrétariat qui peuvent être accompagnés par des investigateurs nommés par le président sur proposition de l'autorité de protection et qui sont soumis aux dispositions de l'article 40. Les agents et les investigateurs sont commissionnés et assermentés à cet effet.

2. Lorsque les investigations ou vérifications portent sur un traitement visé à l'article 61 ou mis en œuvre par le Secrétaire d'État à la Justice, Directeur des Services Judiciaires, par les juridictions et par le ministère public hors de leurs fonctions juridictionnelles, le président de l'autorité de protection désigne le magistrat visé au chiffre 7 de l'article 37 pour procéder auxdites investigations ou vérifications, ou son suppléant en cas d'empêchement. Ce magistrat est accompagné des agents ou investigateurs commissionnés et assermentés mentionnés au chiffre 1 nécessaires à l'exercice de sa mission.

3. Lorsque les investigations ou vérifications portent sur un traitement mis en œuvre par les juridictions et par le ministère public dans l'exercice de leurs fonctions juridictionnelles, le Secrétaire d'Etat à la justice désigne le Délégué judiciaire à la protection des données visé au chiffre 1 de l'article 34 pour procéder auxdites investigations ou vérifications ou son suppléant en cas d'empêchement.

4. Le magistrat visé au chiffre 7 de l'article 37, de même que les agents ou les investigateurs mentionnés aux chiffres 1 et 2 doivent être munis d'une lettre de mission du président de l'autorité de protection précisant expressément le nom et l'adresse de la personne physique ou morale faisant l'objet du contrôle, ainsi que l'objet de la mission.

5. Les opérations de contrôle ne peuvent être effectuées qu'entre 6 et 21 heures ou, en dehors de ces heures, lorsque l'accès au public est autorisé ou lorsqu'une activité est en cours.

Lors desdites opérations, les membres de l'autorité de protection, les agents ou les investigateurs peuvent procéder à toutes vérifications nécessaires, consulter sur place ou sur convocation, tout traitement, demander communication, quel qu'en soit le support, ou prendre copie, par tous moyens, de tout document professionnel et recueillir, auprès de toute personne compétente, les renseignements utiles à leur mission. Ils peuvent accéder aux programmes informatiques et aux informations et en demander la transcription, par tout traitement approprié, dans des documents directement utilisables pour les besoins du contrôle.

6. En dehors des contrôles sur place et sur convocation, les membres de l'autorité de protection, les agents ou les investigateurs peuvent procéder à toute constatation utile ; ils peuvent notamment, à partir d'un service de communication au public en ligne, consulter les données librement accessibles ou rendues accessibles, y compris par imprudence, par négligence ou par le fait d'un tiers, le cas échéant en accédant et en se maintenant dans des systèmes de traitement automatisé d'information le temps nécessaire aux constatations ; ils peuvent retranscrire les données par tout traitement approprié dans des documents directement utilisables pour les besoins du contrôle.

7. Pour mener à bien le contrôle d'un service de communication en ligne, les membres de l'autorité de protection, les agents ou les investigateurs mentionnés au premier alinéa peuvent faire l'usage d'une identité d'emprunt dans les conditions définies par ordonnance souveraine. Cet usage est sans incidence sur la régularité des constations effectuées au titre du présent article.

8. Il est dressé contradictoirement procès-verbal des constatations, vérifications et visites menées en application du présent article. Ce procès-verbal est dressé contradictoirement lorsque les vérifications et visites sont effectuées sur place ou sur convocation. En cas de contrôle en ligne, le procès-verbal de constatation est adressé au responsable du traitement afin qu'il puisse faire valoir ses observations.

Article 44

Dans le cadre des opérations de vérifications et d'investigations visées à l'article 43, le responsable du traitement, le sous-traitant ou toutes personnes interrogées sont tenus de fournir les renseignements demandés et ne peuvent opposer le secret ou une obligation de confidentialité aux membres de l'autorité de protection, à ses agents ou à ses investigateurs.

Toutefois, sont opposables le secret de sécurité nationale, le secret professionnel applicable aux relations entre un avocat et son client ou le secret des sources des traitements journalistiques.

Pour l'exercice des missions visées à l'article 43, l'accès aux traitements relevant de la compétence de l'autorité de protection, qui seraient hébergés dans une zone protégée par le secret de sécurité nationale, est garanti aux membres de l'autorité, agents ou investigateurs visés à l'alinéa premier dudit article.

Le secret médical est également opposable en ce qui concerne les données de santé figurant dans un traitement nécessaire aux fins de la médecine préventive, de la recherche médicale, des diagnostics médicaux, de l'administration de soins ou de traitements, ou de la gestion de service de santé ou des institutions chargées de la médecine du travail ou de la protection sociale. Toutefois la communication des données médicales individuelles incluses dans cette catégorie de traitement est faite à un médecin désigné par le président de l'autorité de protection parmi les médecins figurant sur une liste établie par le Conseil de l'Ordre et comprenant au moins cinq noms.

Le médecin ainsi désigné transmet à l'autorité de protection les seules informations nécessaires aux besoins du contrôle sans faire état, en aucune manière, des informations médicales individuelles auxquelles il a eu accès.

Article 45

Pour l'exercice des missions mentionnées à l'article 43, les membres de l'autorité de protection, ses agents ou ses investigateurs peuvent accéder aux lieux, locaux, enceintes, installations ou établissements servant à la mise en œuvre d'un traitement, à l'exclusion des parties de ceux-ci affectés à l'usage privé, après avoir informé le responsable desdits lieux, locaux, enceintes, installations ou établissements ou son représentant de son droit de s'opposer aux vérifications et investigations. Les opérations de contrôle ont lieu en présence de ce responsable ou de son représentant.

Lorsque le droit de s'opposer aux vérifications et investigations est exercé, les opérations de contrôle ne peuvent avoir lieu qu'après l'autorisation du Président du Tribunal de première instance, saisi sur requête par le président de l'autorité de protection. Le Président du Tribunal statue en tenant compte notamment du motif ou de l'absence de motif justifiant l'opposition.

Toutefois, lorsque l'urgence ou un risque imminent de destruction ou de disparition de pièces ou de documents le justifie, les opérations de vérifications et investigations peuvent avoir lieu sans que le responsable des locaux ou son représentant puisse s'y opposer. Ces opérations peuvent faire l'objet dans tous les cas d'un recours devant le Président du Tribunal de première instance, saisi et statuant comme en matière de référé, lequel prononce leur nullité ainsi que la nullité ou la destruction des preuves recueillies lors de celles-ci, lorsque l'urgence ou le risque imminent n'était pas suffisamment caractérisé au moment du déclenchement desdites opérations.

Article 46

Lorsqu'il existe des raisons de soupçonner que la mise en œuvre des traitements n'est pas conforme aux dispositions de la présente loi, les membres de l'autorité de protection, ses agents ou ses investigateurs peuvent, avec l'autorisation préalable du Président du Tribunal de première instance, saisi par le président de l'autorité de protection, et statuant par ordonnance sur requête, accéder aux lieux, locaux, enceintes, installations ou établissements mentionnés au premier alinéa de l'article 45, y compris les parties de ceux-ci affectées à usage privé sans que le droit d'opposition prévu audit article puisse être exercé.

La requête énonce les éléments de faits et de droit de nature à justifier lesdites opérations de contrôle et à permettre au Président du Tribunal de première instance d'en apprécier le bien-fondé.

L'ordonnance autorisant les opérations de contrôle est exécutoire au seul vu de la minute. Elle peut faire l'objet du recours mentionné à l'article 852 du Code de procédure civile dans le délai de huit jours à compter du contrôle. Ce recours n'est pas suspensif.

Lorsqu'il y est fait droit, le Président du Tribunal de première instance peut déclarer la nullité de ces opérations et des preuves recueillies lors de celles-ci, qui devront être détruites.

L'ensemble de ces opérations a lieu en présence du responsable des lieux, locaux, enceintes, installations ou établissements ou de son représentant ou, en cas d'empêchement ou d'impossibilité, d'au moins un témoin requis à cet effet par les membres de l'autorité de protection, ses agents ou ses investigateurs et ne se trouvant pas placé sous leur autorité.

Article 47

Le président de l'autorité de protection peut signaler à un responsable du traitement ou à son sous-traitant que les opérations de traitement envisagées sont susceptibles de méconnaitre les dispositions de la présente loi.

Lorsqu'un manquement constaté est susceptible de faire l'objet d'une mise en conformité, le président de l'autorité de protection prononce à son égard une mise en demeure, dans le délai qu'il fixe :

1. de satisfaire aux demandes présentées par la personne concernée en vue d'exercer ses droits, dans le respect des dispositions du Chapitre III ;

2. de mettre les opérations de traitement en conformité avec les dispositions de la présente loi ;

3. de communiquer à la personne concernée une violation de données à caractère personnel, à l'exception des traitements visés à l'article 61 ;

4. de rectifier ou d'effacer des données à caractère personnel ou de limiter le traitement de ces données. Dans ce cas, le président de l'autorité de protection peut, dans les mêmes conditions, mettre en demeure le responsable du traitement ou son sous-traitant de notifier aux destinataires des données les mesures qu'il a prises.

Après avoir constaté la mise en conformité, le président de l'autorité de protection prononce la clôture de la procédure de mise en demeure.

Le président peut décider de rendre publique la mise en demeure. Dans ce cas, la décision de clôture de la procédure de mise en demeure fait l'objet de la même publicité.

Article 48

Lorsque la mise en demeure faite au responsable du traitement ou son sous-traitant de se mettre en conformité est demeurée infructueuse ou lorsque le manquement n'est pas susceptible de faire l'objet d'une mise en conformité ou que l'intéressé ne respecte pas les obligations de la présente loi, le président de l'autorité peut, sans avoir à lui adresser la mise en demeure visée à l'article 47, saisir la formation restreinte en vue du prononcé de l'une des sanctions prévues ci-après. Cette saisine s'effectue sur la base d'un rapport établi par l'un des membres de l'autorité de protection, hors formation restreinte, désigné par le président.

Ce rapport est notifié au responsable du traitement ou à son sous-traitant qui peut déposer des observations et se faire représenter ou assister par la personne de son choix.

Le rapporteur peut présenter ses observations à la formation restreinte. Il ne prend pas part à ses délibérations.

Aux fins du prononcé des sanctions, la formation restreinte entend le responsable du traitement, son sous-traitant ou leurs représentants, ainsi que toute personne dont l'audition lui parait susceptible de contribuer utilement à son information, y compris les agents de l'autorité de protection.

À l'issue de cette procédure contradictoire, la formation restreinte peut prononcer à l'encontre de l'entité juridique, personne physique ou morale mise en cause qui assume la responsabilité des traitements ou qui a été qualifiée de sous-traitant l'une ou plusieurs des sanctions suivantes :

1. un avertissement ;

2. une obligation de mettre en conformité le traitement avec les dispositions de la présente loi ou de satisfaire aux demandes présentées par la personne concernée en vue d'exercer ses droits, qui peut être assortie, sauf dans des cas où le traitement est mis en œuvre par l'État ou la Commune, d'une astreinte définitive dont le montant ne peut excéder 1.000 euros par jour de retard calendaire à compter de la date fixée par le président de la formation restreinte ;

3. la limitation temporaire ou définitive du traitement ou son interdiction ;

4. le retrait de l'agrément ou l'injonction, à l'organisme de certification concerné, de refuser une certification ou de retirer la certification accordée ;

5. le retrait de la certification délivrée en vertu de l'article 31 ;

6. la suspension partielle ou totale de la décision d'approbation des règles d'entreprises contraignantes visées à l'article 94 ;

7. la suspension des flux de données adressées à un destinataire situé hors de la Principauté ou à une organisation internationale ;

8. une amende administrative telle que prévue aux articles 50 et 51.

La formation restreinte prend en compte, dans la détermination du montant de l'amende, les critères précisés à l'article 49.

La formation restreinte informe le président de l'autorité de protection des mesures prises au titre des chiffres 1 à 8 susvisés, en vue de leur notification au responsable du traitement ou au sous-traitant.

Ladite formation peut décider de procéder à la publicité des décisions qu'elle prend en application du présent article. Les mesures de publicité peuvent, en cas d'atteinte grave et disproportionnée à la sécurité publique, au respect de la vie privée et familiale ou aux intérêts légitimes des personnes concernées, faire l'objet d'un recours devant le président du Tribunal de première instance, saisi et statuant comme en matière de référé, aux fins qu'il ordonne la suppression de la publication.

Les dispositions des chiffres 3 à 8 ne sont pas applicables à l'État et à la Commune.

Les manquements constitutifs d'infractions pénales sont signalés sans délai au Procureur Général.

Article 49

La formation restreinte de l'autorité de protection prononce, au titre du chiffre 8 de l'article 48, une amende administrative parmi celles prévues aux articles 50 et 51 dont le montant est proportionné à la violation qu'elle sanctionne. A cet effet, elle prend notamment en compte, pour chaque cas d'espèce, les éléments suivants :

- la nature, la gravité et la durée du manquement ;

- le caractère délibéré ou la commission par négligence du manquement, ou de sa répétition;

- les mesures prises par le responsable du traitement ou le sous-traitant pour atténuer le dommage subi par les personnes concernées ;

- le degré de coopération avec l'autorité de protection en vue de remédier à la violation et d'en atténuer les éventuels effets négatifs ;

- les catégories de données à caractère personnel concernées par la violation ;

- les éventuelles circonstances aggravantes ou atténuantes applicables au cas d'espèce.

Article 50

Est puni d'une amende administrative ne pouvant excéder 500.000 euros, le manquement aux obligations relatives :

- à la vérification de l'obtention du consentement prévu à l'article 6 ;

- à la coopération avec l'autorité de protection prévue à l'article 21 ;

- à la protection par défaut et à la protection dès la conception prévue à l'article 22 ;

- aux exigences en matière de responsabilité conjointe, de désignation d'un représentant, de sous-traitance, de tenue du registre ou de désignation d'un délégué à la protection des données prévues aux articles 23 à 27 ;

- aux mesures de sécurité des traitements prévues à l'article 28 ;

- à la notification des violations de données à caractère personnel à l'autorité de protection et, le cas échéant, la communication à la personne concernée dans les conditions prévues à l'article 29 ;

- aux codes de conduite prévus à l'article 30 :

- aux exigences en matière d'analyses d'impact prévues aux articles 32 et 33 ;

- à l'information de l'autorité de protection de l'existence d'un système de vidéosurveillance tel que prévu par le second alinéa de l'article 82.

Article 51

Est puni d'une amende administrative ne pouvant excéder 900.000 euros, le manquement aux obligations relatives :

- aux caractéristiques des données à caractère personnel, à la licéité du traitement, au consentement et à l'information visés respectivement aux articles 4, 5, 6 et 84 ;

- à l'information des personnes concernées en application de l'article 10 ;

- à la collecte, l'enregistrement, la conservation ou l'utilisation de données sensibles, sauf les dérogations prévues par la loi ;

- aux droits des personnes concernées visés aux articles 11 à 19 ;

- à la communication de renseignements ou documents inexacts soit aux personnes concernées soit à celles chargées d'effectuer les vérifications ou investigations ;

- à l'exception des autorités administratives et judiciaires compétentes, à la collecte, l'enregistrement, la conservation ou l'utilisation de données à caractère personnel concernant des infractions, des condamnations ou des mesures de sûreté ou qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté ;

- aux transferts de données à caractère personnel hors de la Principauté sans respecter les dispositions prévues aux articles 92 à 97.

- à la méconnaissance des injonctions et des prescriptions prononcées par la formation restreinte de l'autorité de protection des données personnelles en vertu de l'article 48.

Article 52

Les amendes administratives et, après liquidation par le président de la formation restreinte de l'autorité de protection, les astreintes visées à l'article 48 sont à régler à la Trésorerie Générale des Finances de la Principauté dans un délai de trois mois suivant la date de leur notification et portent intérêt au taux légal à l'expiration de ce délai.

Article 53

Lorsque le non-respect des dispositions de la présente loi entraine une violation des libertés et droits fondamentaux visés à l'article premier et que l'urgence le justifie le président de l'autorité de protection saisit la formation restreinte qui, après procédure contradictoire, définie par ordonnance souveraine, peut prendre une mesure provisoire de suspension du traitement ou toute mesure conservatoire, qui ne peut excéder un délai de 6 mois.

En cas d'atteinte grave et immédiate aux droits et libertés mentionnés à l'article premier de la présente loi, le président de l'Autorité de protection peut en outre demander, par la voie du référé, au Président du Tribunal de première instance d'ordonner, le cas échéant sous astreinte, toute mesure nécessaire à la sauvegarde de ces droits et libertés.

Article 54

Les décisions de la formation restreinte de l'autorité de protection prises en application des dispositions de l'article 48 sont susceptibles de recours de plein contentieux devant le Tribunal de première instance.

CHAPITRE VI - TRAITEMENTS SOUMIS A FORMALITES PREALABLES

Article 55

Sont soumis à l'avis de l'autorité de protection :

1. les traitements mis en œuvre à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces visés à l'article 61 ;

2. les traitements portant sur des données génétiques ou biométriques visés à l'article 74 ;

3. les traitements relatifs à la recherche dans le domaine de la santé visés aux articles 75 et 76.

Sont soumis à l'autorisation de l'autorité de protection les transferts de données à caractère personnel visés à l'article 96.

Section I – Dispositions communes

Article 56

Les traitements visés aux articles 61 et 74 ne peuvent être mis en œuvre que par les autorités administratives et judiciaires compétentes dans le cadre exclusif des missions qui leur sont légalement conférées.

A l'exception des traitements mis en œuvre par l'autorité judiciaire pour les besoins des procédures diligentées devant les diverses juridictions et des procédures d'entraide judiciaire internationale, les traitements visés à l'article 55 font l'objet d'une demande d'avis ou d'une demande d'autorisation auprès de l'autorité de protection.

Les traitements visés aux articles 61 et 74 sont autorisés par arrêté ministériel ou par arrêté du Secrétaire d'Etat à la Justice, Directeur des Services Judiciaires. L'arrêté et l'avis motivé qui l'accompagne font l'objet d'une publication au Journal de Monaco. Pour les traitements visés à l'article 61, l'avis fait l'objet d'une publication sauf décision motivée du Ministre d'Etat. Dans ce cas, seul est publié le sens de l'avis.

L'avis est rendu dans un délai de deux mois à compter du dépôt du dossier comportant les mentions visées à l'article 57.

Le délai prévu à l'alinéa précédent peut être renouvelé une fois sur décision motivée du président de l'autorité de protection. Lorsqu'il n'est pas rendu à l'expiration du délai précité, l'avis est réputé favorable.

Article 57

Les demandes d'avis et les demandes d'autorisation adressées à l'autorité de protection sont recevables dès lors qu'elles comportent les mentions suivantes :

1. le nom et les coordonnées professionnelles du responsable du traitement ou son représentant à Monaco ;

2. le fondement juridique du traitement et, le cas échéant, le projet d'arrêté ministériel ou le projet d'arrêté du Secrétaire d'Etat à la Justice, Directeur des Services Judiciaires ;

3. la ou les finalités du traitement ;

4. la dénomination du traitement s'il y a lieu ;

5. les catégories de données à caractère personnel traitées, leur origine et les catégories de personnes concernées par le traitement ;

6. la durée de conservation des données à caractère personnel traitées ou, en cas d'impossibilité, les critères utilisés pour déterminer cette durée ;

7. le ou les services chargés de la mise en œuvre du traitement ;

8. l'analyse des risques relative à la sécurité des traitements y compris les mesures de sécurité ;

9. l'autorité ou la fonction de la personne ou le service auprès de laquelle s'exerce le droit d'accès ainsi que les mesures prises pour faciliter l'exercice de ce droit ;

10. les catégories de personnes qui, à raison de leurs fonctions ou pour les besoins du service, ont accès aux données à caractère personnel enregistrées ;

11. les destinataires ou catégories de destinataires habilités à recevoir communication des données à caractère personnel ;

12. le cas échéant, les interconnexions, les rapprochements ou toute autre forme de mise en relation avec d'autres traitements ;

13. le cas échéant, l'identité et l'adresse du sous-traitant ;

14. le cas échéant, les transferts de données hors de la Principauté et les garanties appropriées encadrant lesdits transferts.

Article 58

L'autorité de protection est tenue informée de tout changement affectant les informations visées à l'article 57 et de la suppression du traitement.

Article 59

L'arrêté ministériel et l'arrêté du Secrétaire d'Etat à la Justice, Directeur des Services Judiciaires visés à l'article 56 portant autorisation du traitement précisent :

- la dénomination et la finalité du traitement ;

- les catégories de données à caractère personnel enregistrées ;

- les destinataires ou catégories de destinataires habilités à recevoir les données à caractère personnel ;

- le cas échéant, les dérogations prévues à l'article 20 de la présente loi.

Article 60

L'autorité de protection tient à la disposition du public la liste des traitements ayant fait l'objet d'une des formalités prévues à l'article 55.

Section II - Traitements mis en œuvre à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces

Article 61

Les traitements mis en œuvre à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces, sont régis par les dispositions de la présente section et, sous réserve de leur compatibilité avec ces dernières, par les autres dispositions de la présente loi.

Ces traitements ne sont licites que s'ils sont fondés sur une disposition législative ou réglementaire et dans la mesure où ils sont nécessaires à l'exécution d'une mission effectuée pour l'une des finalités énoncées au précédent alinéa par les autorités administratives et judiciaires compétentes.

Article 62

Les données à caractère personnel collectées par les autorités administratives et judiciaires visées à l'article 56 pour l'une des finalités énoncées à l'article 61 ne peuvent être traitées pour d'autres finalités qu'en application d'une disposition législative ou réglementaire ou d'engagements internationaux rendus exécutoires dans la Principauté.

Article 63

Les traitements effectués pour l'une des finalités énoncées à l'article 61 autre que celles pour lesquelles les données personnelles ont été collectées peuvent être mis en œuvre s'ils sont nécessaires et proportionnés à cette finalité, sous réserve de garanties appropriées.

Ces traitements peuvent comprendre l'archivage dans l'intérêt public, à des fins scientifiques, statistiques ou historiques.

Article 64

Toute décision fondée exclusivement sur un traitement automatisé, y compris le profilage, qui produit des effets juridiques défavorables pour la personne concernée ou l'affecte de manière significative, est interdite, à moins qu'elle ne soit autorisée par arrêté ministériel ou par arrêté du Secrétaire d'Etat à la Justice, Directeur des Services Judiciaires, pris après avis de l'autorité de protection, et que le responsable du traitement fournisse des garanties appropriées pour les droits et libertés de la personne concernée et au minimum le droit d'obtenir une intervention humaine, notamment lorsqu'elle souhaite exprimer son point de vue, obtenir une explication quant à la décision prise ou contester la décision.

Cette décision ne peut être fondée sur des données sensibles à moins que des mesures appropriées pour la sauvegarde des droits et des libertés et des intérêts légitimes de la personne concernée n'aient été prises.

Tout profilage qui entraîne une discrimination à l'égard des personnes concernées sur la base de données sensibles est interdit.

Article 65

Le responsable du traitement prend les mesures raisonnables pour garantir que les données à caractère personnel qui sont inexactes, incomplètes ou ne sont plus à jour soient effacées, rectifiées ou complétées.

Toute transmission de données à caractère personnel doit, dans la mesure du possible, être complétée d'informations permettant au destinataire de juger de l'exactitude, de l'exhaustivité et de la fiabilité des données à caractère personnel et de leur niveau de mise à jour.

S'il s'avère que des données à caractère personnel inexactes ont été transmises ou que des données à caractère personnel ont été transmises de manière illicite, le destinataire en est informé dans les meilleurs délais par le responsable du traitement, dès que ce dernier en a eu connaissance. Dans ce cas, les données à caractère personnel sont rectifiées ou effacées.

Article 66

Le responsable du traitement établit, dans la mesure du possible et le cas échéant, une distinction claire entre les différentes catégories de personnes concernées par le traitement, telles que :

1. les personnes à l'égard desquelles il existe des motifs sérieux de croire qu'elles ont commis ou sont sur le point de commettre une infraction pénale ;

2. les personnes reconnues coupables d'une infraction pénale ;

3. les victimes d'une infraction pénale ou les personnes à l'égard desquelles certains faits portent à croire qu'elles pourraient être victimes d'une infraction pénale ;

4. les personnes autres que celles mentionnées aux chiffres 1, 2 et 3 ci-dessus, telles que celles pouvant être appelées à témoigner lors d'enquêtes en rapport avec des infractions pénales ou des procédures pénales ultérieures, des personnes pouvant fournir des informations sur des infractions pénales ou des contacts ou des associés de l'une des personnes mentionnées aux chiffres 1 et 2.

Les données à caractère personnel fondées sur des faits sont, dans la mesure du possible, distinguées de celles fondées sur des appréciations personnelles.

Article 67

Le responsable du traitement ou son sous-traitant établit pour chaque traitement automatisé un journal des opérations de collecte, de modification, de consultation et de communication, y compris les transferts, l'interconnexion et l'effacement, portant sur de telles données.

Les journaux des opérations de consultation et de communication permettent d'en établir le motif, la date et l'heure. Ils permettent également, dans la mesure du possible d'identifier les personnes qui consultent ou communiquent les données et les destinataires de celles-ci.

Ce journal est exclusivement utilisé à des fins de vérification de la licéité des opérations du traitement, d'autocontrôle, de garantie de l'intégrité et de la sécurité des données et à des fins de procédures pénales.

Il est mis à la disposition de l’autorité de protection à sa demande.

Article 68

Par dérogation à l’article 9, le responsable du traitement prend les mesures raisonnables pour fournir toute information et procéder à toute mesure relative à l’exercice des droits de la personne concernée de façon concise, compréhensible et aisément accessible. Les informations sont fournies gratuitement par tout moyen approprié. Il informe la personne concernée des suites données à sa demande dans les meilleurs délais.

Article 69

Par dérogation à l’article 10, le responsable du traitement met à la disposition de la personne concernée les informations suivantes :

- le nom et les coordonnées professionnelles du responsable du traitement ;

- le cas échéant les coordonnées professionnelles du délégué à la protection des données ;

- les finalités du traitement ;

- le droit d'introduire une réclamation auprès de l'autorité de protection ;

- l'existence d'un droit d'accès, de rectification ou d'effacement ;

- le fondement juridique du traitement ;

- la durée de conservation des données à caractère personnel ou lorsque ce n'est pas possible les critères utilisés pour déterminer cette durée ;

- le cas échéant, les catégories de destinataires ;

- au besoin, des informations complémentaires, en particulier lorsque les données à caractère personnel sont collectées à l'insu de la personne concernée ;

- le droit d'introduire une réclamation auprès de l'autorité de protection ;

- l'existence d'un droit d'accès, de rectification ou d'effacement.

Le responsable du traitement peut décider de retarder, limiter ou ne pas fournir ces informations pour éviter de porter atteinte aux enquêtes, recherches ou procédures officielles ou judiciaires en cours, de nuire à la prévention ou à la détection d'infractions pénales, aux enquêtes ou aux poursuites en la matière ou à l'exécution de sanctions pénales, à la sécurité publique ou à la sécurité nationale ou pour protéger les droits et liberté d'autrui, dès lors et aussi longtemps qu'une telle décision est nécessaire et proportionnée et tient compte des droits et intérêts des personnes concernées.

Article 70

Par dérogation au dernier alinéa de l'article 29, la communication d'une violation de données à caractère personnel à la personne concernée peut être retardée, limitée ou ne pas être délivrée par le responsable du traitement pour éviter de gêner des enquêtes, des recherches ou des procédures administratives ou judiciaires, pour éviter de nuire à la prévention ou à la détection d'infractions pénales, aux enquêtes ou aux poursuites en la matière ou à l'exécution de sanctions pénales, pour protéger la sécurité publique, pour protéger la sécurité nationale ou pour protéger les droits et libertés d'autrui.

Article 71

Le droit d'accès prévu à l'article 11 s'exerce auprès de l'autorité de protection.

La personne concernée par un traitement relevant de l'article 61 peut saisir l'autorité de protection d'une demande de vérification pour savoir si ses données font l'objet d'un traitement.

Lorsque l'autorité de protection est saisie, le président désigne le magistrat visé au chiffre 7 de l'article 37 ou, en cas d'empêchement de celui-ci, le magistrat suppléant pour effectuer toutes les vérifications. Celui-ci peut se faire assister d'un agent de l'autorité de protection dûment commissionné et assermenté. A l'issue de ces vérifications, le président de l'autorité de protection met en demeure le responsable du traitement, s'il y a lieu, de procéder aux modifications nécessaires.

Le président de l'autorité de protection informe la personne concernée que les vérifications ont été effectuées. Avec l'accord du responsable du traitement, il peut porter à sa connaissance les informations dont la communication ne porte pas atteinte aux enquêtes ou procédures judiciaires en cours, à la sécurité publique ou à la préservation de la sécurité nationale.

En cas de refus de communication pour les motifs susvisés, l'autorité de protection indique à la personne concernée ses voies de recours.

Article 72

Le droit de rectification et le droit d'effacement prévus aux articles 12 et 13 de la présente loi s'exercent auprès du responsable du traitement.

La personne concernée par un traitement relevant de l'article 61 peut saisir le responsable du traitement d'une demande de rectification ou d'effacement de ses données.

A l'appui de sa demande, la personne concernée produit toutes pièces justificatives utiles, et notamment la copie des éventuelles décisions de classement sans suite, de non-lieu, de relaxe ou d'acquittement afin :

1. que soient rectifiées les données à caractère personnel la concernant qui sont inexactes ;

2. que soient complétées les données à caractère personnel la concernant incomplètes ;

3. que soient effacées les données à caractère personnel la concernant en cas d'erreur manifeste.

Si la demande de rectification ou d'effacement est susceptible de porter atteinte aux enquêtes ou procédures judiciaires en cours, à la sécurité publique ou à la préservation de la sécurité nationale, le responsable du traitement lorsqu'il est saisi, informe la personne concernée du refus de procéder à la rectification ou à l'effacement de ses données ainsi que de ses voies de recours.

Lorsque des données à caractère personnel ont été rectifiées ou effacées au titre du présent article, le responsable du traitement adresse une notification aux destinataires afin que ceux-ci rectifient ou effacent les données à caractère personnel sous leur responsabilité.

Article 73

1. Sans préjudice de l'article 93, le transfert de données à caractère personnel relatif aux traitements relevant de la présente section vers un Etat ou une organisation internationale n'assurant pas un niveau de protection des données adéquat, peut toutefois s'effectuer lorsque :

a) des garanties appropriées sont offertes dans un instrument juridiquement contraignant exécutoire dans la Principauté et dans l'Etat ou l'organisation internationale destinataire et assurant la protection des données à caractère personnel, notamment le droit à un recours effectif ou

b) l'analyse de toutes les circonstances du transfert permet d'estimer qu'il existe des garanties appropriées en matière de protection des données à caractère personnel.

2. En l'absence de niveau adéquat de protection des données à caractère personnel au sens de l'article 93 ou de garanties visées au chiffre 1 du présent article, le transfert peut s'effectuer :

a) s'il est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'autres personnes, lorsque la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement ;

b) pour la sauvegarde des intérêts légitimes de la personne concernée lorsque le droit de l'État transférant les données à caractère personnel le prévoit ;

c) pour prévenir une menace grave et immédiate pour la sécurité publique ou préserver les intérêts fondamentaux de l'Etat ;

d) s'il est nécessaire à la constatation, l'exercice ou la défense d'un droit en justice.

3. Nonobstant le niveau de protection de l'Etat ou de l'organisation internationale vers lequel s'opère le transfert, des limites peuvent être fixées au transfert de catégories spécifiques de données pour des motifs importants d'intérêt public.

4. Sans préjudice des chiffres 1 à 3 du présent article, le transfert de données à caractère personnel relatif aux traitements relevant de la présente section ne peut s'effectuer, hors de la Principauté, qu'auprès d'une autorité publique ou de tout autre organisme ou entité à qui a été confié l'exercice de l'autorité publique et des prérogatives de puissance publique et que si le transfert est nécessaire aux fins énoncées à l'article 61 ou, du fait du renvoi opéré par l'article 91, aux fins énoncées au chiffre 2 du quatrième alinéa de l'article 34, c'est-à-dire pour les traitements qui intéressent la sécurité nationale mis en œuvre dans le cadre des articles 9 à 15 et 18 de la loi n°1.430 du 13 juillet 2016, précitée.

5. Le transfert, hors de la Principauté, de données à caractère personnel provenant d'un autre État ne peut s'effectuer que si ledit État a donné son accord préalable à ce transfert. Toutefois, si cet accord ne peut être obtenu en temps utile, ces données peuvent être transmises vers un autre État lorsque cette nouvelle transmission est nécessaire à la prévention d'une menace grave et immédiate pour la sécurité publique d'un autre État ou pour la sauvegarde des intérêts fondamentaux de la Principauté. L'autorité publique, l'organisme ou l'entité dont provenaient ces données en est informée sans retard.

6. Un transfert ultérieur vers un autre Etat ou vers une organisation internationale peut, en l'absence de l'accord mentionné à l' alinéa précédent, être autorisé par l'autorité publique compétente au regard de facteurs pertinents, y compris la finalité pour laquelle les données à caractère personnel ont été transférées initialement, le niveau de protection des données à caractère personnel dans l'Etat ou au sein de l'organisation internationale vers lesquels les données à caractère personnel sont transférées ultérieurement et la gravité de l'infraction pénale, ou, du fait du renvoi au présent article par l'article 91, pour la préservation de la sécurité nationale.

Section III - Traitements à caractère personnel relatifs aux données génétiques ou biométriques

Article 74

Les traitements mis en œuvre par les autorités administratives et judiciaires, agissant dans le cadre de leurs prérogatives de puissance publique, qui portent sur des données génétiques ou sur des données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes sont soumis à l'avis de l'autorité de protection dans les conditions prévues à l'article 56.

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

Si le traitement est mis en œuvre pour l'une des finalités énoncées à l'article 61, le transfert des données s'effectue dans les conditions prévues à l'article 73.

Section IV - Traitements relatifs à la recherche dans le domaine de la santé

Article 75

Sous réserve des dispositions de l'article 76, le traitement ayant pour fin la recherche dans le domaine de la santé est mis en œuvre après avis motivé de l'autorité de protection dans les conditions prévues aux articles 57 et 58.

Préalablement au prononcé de cet avis, l'autorité de protection peut, dans des conditions fixées par ordonnance souveraine, consulter un service public compétent dans le domaine de la santé.

Cette consultation suspend le délai visé au quatrième alinéa de l'article 56.

Article 76

Le traitement devant être effectué dans le cadre d'une recherche impliquant la personne humaine, au sens de la législation relative à la protection des personnes se prêtant à la recherche biomédicale, ne peut être mis en œuvre qu'après avis de l'autorité de protection dans les conditions prévues aux articles 57 et 58.

Le dossier produit à l'appui de la demande d'avis comporte, en sus des éléments prévus à l'article 57, la mention de l'objectif de la recherche, de la population concernée, de la méthode d'observation ou d'investigation retenue, de la justification du recours aux données à caractère personnel traitées, de la durée et des modalités d'organisation de la recherche, de la méthode d'analyse des données, ainsi que, le cas échéant, une copie de l'avis émis par le comité compétent en application de la législation mentionnée à l'alinéa précédent.

L'autorité de protection n'est pas compétente pour apprécier la qualification d'une recherche impliquant la personne humaine.

CHAPITRE VII - DISPOSITIONS PARTICULIERES A CERTAINS TRAITEMENTS

Section I - Traitements relatifs aux infractions, condamnations pénales et mesures de sûreté ou portant sur des soupçons d'activités illicites

Article 77

Les traitements relatifs aux infractions, aux condamnations pénales, mesures de sûreté ou portant sur des soupçons d'activités illicites peuvent être mis en œuvre, sous réserve de garanties appropriées, par :

1. les personnes morales de droit public et les organismes de droit privé investis d'une mission d'intérêt général ou concessionnaires d'un service public, agissant dans le cadre de leurs attributions légales ;

2. les personnes physiques et morales de droit privé collaborant au service public de la justice, et appartenant à des catégories dont la liste est fixée par arrêté du Secrétaire d'Etat à la Justice, Directeur des Services Judicaires pris après avis de l'autorité de protection dans la mesure strictement nécessaire à leur mission ;

3. les auxiliaires de justice, pour les stricts besoins de l'exercice des missions qui leur sont confiées par la loi ;

4. les personnes physiques ou morales de droit privé agissant dans le cadre de leurs obligations légales ;

5. les personnes physiques ou morales victimes ou mises en cause dans une procédure judiciaire, aux fins de leur permettre de préparer et, le cas échéant, d'exercer et de suivre une action en justice pour une durée strictement proportionnée à cette finalité.

Section II - Traitements à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique, ou à des fins statistiques

Article 78

Les traitements à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique, ou à des fins statistiques sont soumis à des garanties appropriées pour les droits et libertés de la personne concernée.

Les droits visés aux articles 11, 12, 14, 15, 16 et 17 ne sont pas applicables aux traitements mis en œuvre à des fins archivistiques dans l'intérêt public, lorsque l'exercice de ces droits risquerait de rendre impossible ou d'entraver sérieusement la réalisation des finalités pour lesquelles les données à caractère personnel sont collectées.

Les droits visés aux articles 11, 12, 14 et 16 ne sont pas applicables aux traitements mis en œuvre à des fins de recherche scientifique ou historique ou à des fins statistiques lorsque l'exercice de ces droits risquerait de rendre impossible ou d'entraver sérieusement la réalisation des finalités pour lesquelles les données à caractère personnel sont collectées.

Section III - Traitements relatifs à la liberté d'expression

Article 79

Aux fins de concilier la protection des données à caractère personnel et la liberté d'expression, il peut être dérogé, indépendamment des dispositions prévues à l'article 20, aux dispositions prévues au chiffre 5 de l'article 4, aux articles 7, 10, 11, 12, 14, 77, 90, et 93 à 95, lorsque le traitement est effectué à des fins journalistiques ou à des fins de liberté d'expression notamment l'expression universitaire, artistique ou littéraire.

Section IV - Traitements relatifs à la vidéosurveillance

Article 80

Des systèmes de vidéosurveillance peuvent être installés dans des lieux ouverts ou non au public à des fins de sécurité des biens et des personnes.

Au sens de la présente loi, on entend par système de vidéosurveillance toute opération consistant en la captation, la transmission, l'enregistrement et l'exploitation d'images prises en tout lieu, qu'il soit public, ouvert au public ou privé, par une personne physique ou morale de droit privé ou une personne morale de droit public agissant en dehors de l'exercice de ses prérogatives de puissance publique.

Article 81

Sans préjudice des dispositions de l'article 10, l'information du public de la présence d'un système de vidéosurveillance dans des lieux ouverts au public est réalisée par le responsable du traitement de façon visible et permanente au moyen d'un panneau placé à l'extérieur des lieux concernés.

L'information de la personne concernée de la présence d'un système de vidéosurveillance dans des lieux non ouverts au public est réalisée par le responsable du traitement de façon visible et permanente au moyen d'un panneau placé à l'intérieur des lieux concernés ou par une information appropriée des personnes concernées.

Le panneau comporte au minimum les informations relatives aux finalités du traitement, à l'identité du responsable du traitement et à l'exercice des droits de la personne concernée.

La conservation des images issues des systèmes de vidéosurveillance ne doit pas excéder 30 jours.

Seules les personnes dûment autorisées dans le cadre de leurs fonctions peuvent visualiser et enregistrer les images.

Article 82

Les systèmes de vidéosurveillance installés dans des lieux ouverts au public ou filmant les abords de voies publiques, d'espaces ouverts au public ou à la circulation du public, sont soumis à l'autorisation préalable du Ministre d'État.

Les systèmes de vidéosurveillance installés dans les lieux non ouverts au public sont portés à la connaissance de l'autorité de protection.

Article 83

Les modalités d'application de la présente section sont définies par arrêté ministériel.

Section V - Traitements dans le secteur des communications électroniques

Article 84

L'utilisation de réseaux de communications électroniques en vue d'accéder ou de collecter des données à caractère personnel conservées dans l'équipement terminal d'un abonné ou d'un utilisateur est précédée d'une information claire et complète de l'utilisateur ou de l'abonné, sur la finalité du traitement et sur les moyens dont il dispose pour s'y opposer.

Sont qualifiés de réseaux de communications électroniques les systèmes de transmission et, le cas échéant, les équipements de commutation ou de routage ainsi que les autres ressources qui permettent l'acheminement de signaux par câble, par voie hertzienne, par moyen optique ou par d'autres moyens électromagnétiques.

Il est interdit de subordonner l'accès à un service disponible sur un réseau de communications électroniques à l'acceptation, par l'abonné ou l'utilisateur concerné, du traitement des données stockées dans son équipement terminal, sauf si la conservation ou l'accès technique visent exclusivement à effectuer ou à faciliter la transmission d'une communication par la voie d'un réseau de communications électroniques, ou sont strictement nécessaires à la fourniture d'un service expressément demandé par l'abonné ou l'utilisateur.

Section VI - Traitements mis en œuvre dans le cadre des dispositions des articles 9 à 15 et 18 de la loi n°1.430 du 13 juillet 2016 portant diverses mesures relatives à la préservation de la sécurité nationale

Article 85

Au quatrième alinéa de l'article 16 de la loi n° 1.430 du 13 juillet 2016, précitée, les mots « *d'un an* » sont remplacés par les mots « *de cinq ans qui commence à courir, pour les membres visés au chiffre 2, à compter du onzième jour après l'élection du Conseil National* ».

Article 86

La commission instituée par l'article 16 de la loi n° 1.430 du 13 juillet 2016, précitée, est également chargée de contrôler, en toute indépendance, les traitements mis en œuvre dans le cadre des articles 9 à 15 et 18 de ladite loi conformément à ses dispositions ainsi qu'à celles de la présente loi en matière de protection des données personnelles applicable à ces traitements.

Article 87

Les traitements qui intéressent la sécurité nationale visés au chiffre 2 du quatrième alinéa de l'article 34 sont régis par les dispositions de la présente section et, sous réserve de leur compatibilité avec ces dernières, par les autres dispositions de la présente loi.

Ces traitements ne sont licites que s'ils sont fondés sur une disposition législative ou réglementaire et dans la mesure où ils sont nécessaires à l'exécution d'une mission effectuée pour l'une des finalités énoncées au précédent alinéa par les autorités administratives compétentes dans le cadre exclusif des missions qui leur sont conférées par la loi n° 1.430 du 13 juillet 2016, précitée.

Article 88

Les traitements visés à l'article précédent font l'objet d'une demande d'avis auprès de la commission instituée par l'article 16 de la loi n° 1.430 du 13 juillet 2016, précitée. La demande d'avis contient les informations visées à l'article 57 de la présente loi.

L'avis est rendu dans un délai de deux mois à compter du dépôt du dossier comportant lesdites informations.

Le délai prévu à l'alinéa précédent peut être renouvelé une fois sur décision motivée du président de la commission. Lorsqu'il n'est pas rendu à l'expiration du délai précité, l'avis est réputé favorable.

La commission est informée de tout changement affectant les informations visées à l'article 57 et de la suppression du traitement.

Les traitements visés au premier alinéa sont autorisés par arrêté ministériel.

L'arrêté ministériel portant autorisation du traitement précise les informations visées à l'article 59.

Cet arrêté ministériel portant autorisation du traitement ainsi que l'avis préalable qui l'accompagne sont dispensés de publication au Journal de Monaco.

Article 89

1. Le contrôle de la mise en œuvre des traitements est assuré par la même commission, laquelle vérifie que les données personnelles sont collectées et traitées dans le respect des dispositions de la présente loi.

A cette fin, elle peut accéder aux données de ces traitements sous réserve des nécessités de la protection des sources et de la protection des données communiquées par les services de renseignements étrangers.

2. En cas d'irrégularités constatées, le président de la commission saisit le Ministre d'Etat pour qu'il prenne toutes mesures afin de faire cesser lesdites irrégularités ou pour que leurs effets soient supprimés. Sous réserve des dispositions relatives au secret de sécurité nationale, la Commission peut rendre compte publiquement et périodiquement de ses activités de contrôle au titre de la présente loi.

Article 90

Toute personne ayant un intérêt direct et personnel peut exercer auprès de la commission ses droits d'accès, de rectification et d'effacement dans les conditions suivantes.

A cet effet, elle saisit la commission soit d'une demande de vérification pour savoir si ses données font l'objet d'un traitement, soit d'une demande de rectification ou d'effacement de ses données. Dans ces deux derniers cas, elle produit à l'appui de sa demande, toute pièce justificative utile afin :

1. que soient rectifiées les données à caractère personnel la concernant qui sont inexactes ;
2. que soient complétées les données à caractère personnel la concernant incomplètes ;
3. que soient effacées les données à caractère personnel la concernant en cas d'erreur manifeste.

Si la Commission considère qu'il peut être fait droit à la demande de rectification ou d'effacement, le président de la commission saisit le Ministre d'Etat afin qu'il prenne toutes mesures pour y procéder.

Dans tous les cas, la commission notifie à la personne auteur de la demande que les vérifications nécessaires ont été effectuées, sans jamais confirmer ou infirmer la mise en œuvre de l'une des opérations de police administrative visées par les articles 9 à 15 de la loi n° 1.430 du 13 juillet 2016, précitée, ou d'un traitement institué dans le cadre de l'article 18 de cette loi.

Article 91

Les transferts de données hors de la Principauté s'effectuent dans les conditions prévues à l'article 73 de la présente loi.

Article 92

Les crédits nécessaires au fonctionnement de la commission instituée par l'article 16 de la loi n° 1.430 du 13 juillet 2016, précitée, sont inscrits dans un chapitre spécifique du budget de l'Etat.

CHAPITRE VIII - TRANSFERT DES DONNEES A CARACTERE PERSONNEL

Article 93

Des données à caractère personnel peuvent être transférées à l'étranger si la Principauté a constaté que l'Etat ou l'organisation internationale vers lesquels s'opère ledit transfert dispose d'une législation ou d'une règlementation présentant un niveau de protection adéquat bénéficiant notamment aux personnes concernées dont les données sont collectées dans la Principauté.

La liste des États et organisations internationales disposant du niveau de protection visé à l'alinéa précédent est adoptée par arrêté ministériel, après avis de l'autorité de protection. Elle est régulièrement mise à jour et publiée au Journal de Monaco et sur le site internet de l'autorité de protection.

Article 94

Le transfert de données à caractère personnel vers un État ou une organisation internationale n'assurant pas, au sens de l'article 93 un niveau de protection adéquat, peut toutefois s'effectuer s'il est garanti par :

- le respect d'un engagement international exécutoire dans la Principauté ;

- l'utilisation de clauses types de protection préalablement approuvées par l'autorité de protection ;

- le respect des règles d'entreprises contraignantes approuvées par l'autorité de protection ou par une autorité chargée de la protection des données relevant d'un Etat qui assure un niveau de protection adéquat,

- un mécanisme de certification approuvé conformément aux dispositions de l'article 31 ;

- l'adhésion à un code de conduite approuvé et publié par l'autorité de protection.

Article 95

1. En l'absence de niveau de protection adéquat prévu à l'article 93 ou de garanties appropriées visées à l'article 94, le transfert de données peut toutefois s'effectuer si la personne à laquelle se rapportent les données a explicitement consenti à leur transfert après avoir été informée de l'absence du niveau de protection ou de garanties appropriées.

2. Le transfert de données peut également s'effectuer :

a) s'il est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'autres personnes, lorsque la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement ;

b) pour des motifs importants d'intérêt public ;

c) s'il est nécessaire à la constatation, l'exercice ou la défense d'un droit en justice ;

d) pour la consultation d'un registre public prévu par la loi destiné à l'information du public et ouvert à la consultation de celui-ci ou de toute personne justifiant d'un intérêt légitime ;

e) s'il est nécessaire à l'exécution d'un contrat entre le responsable du traitement ou son représentant et la personne concernée ou à la mise en œuvre de mesures précontractuelles prises à la demande de la personne concernée ;

f) s'il est nécessaire à la conclusion ou à l'exécution d'un contrat conclu ou à conclure, dans l'intérêt de la personne concernée, entre le responsable du traitement ou son représentant et un tiers.

L'autorité de protection peut obtenir de la part du responsable du traitement ou du sous-traitant toute information pertinente relative aux transferts de données personnelles lorsqu'ils sont effectués pour des motifs importants d'intérêt public.

3. Si le transfert ne peut être fondé sur les dispositions de l'article 93 ou 94 et qu'aucune des dérogations prévues aux chiffres 1 et 2 du présent article n'est applicable, un transfert hors de la Principauté peut avoir lieu s'il ne revêt pas de caractère répétitif, s'il ne touche qu'un nombre limité de personnes, s'il est nécessaire aux fins d'intérêts légitimes impérieux poursuivis par le responsable du traitement et que des garanties appropriées ont été prises. Le responsable du traitement informe l'autorité de protection de ce transfert.

Les chiffres 1 et 3, ainsi que les lettres e) et f) du chiffre 2 du présent article ne sont pas applicables aux activités des autorités publiques dans l'exercice de leurs prérogatives de puissance publique.

4. Nonobstant le niveau de protection de l'Etat ou de l'organisation internationale vers lequel s'opère le transfert, des limites peuvent être fixées au transfert de catégories spécifiques de données pour des motifs importants d'intérêt public.

Article 96

Le transfert de données à caractère personnel vers un État ou une organisation internationale ne répondant pas aux exigences fixées aux articles 93 à 95 peut toutefois s'effectuer avec l'autorisation de l'autorité de protection sur la base de mesures de protection particulières ou de clauses contractuelles spécifiques entre le responsable du traitement et le sous-traitant ou entre l'un de ceux-ci et le responsable du traitement, le sous-traitant et le destinataire de ces données.

L'autorité de protection des données personnelles se prononce dans un délai de deux mois à compter de la réception de la demande. Ce délai peut être renouvelé une fois sur décision motivée du président.

L'autorisation demandée à l'autorité de protection sur le transfert mentionné au premier alinéa qui n'est pas délivrée à l'expiration du délai mentionné ci-dessus, est réputée refusée.

Article 97

Le transfert ou la divulgation de données à caractère personnel hors de la Principauté fondé sur une décision d'une juridiction ou d'une autorité administrative exigeant d'un responsable du traitement ou d'un sous-traitant un tel transfert ou une telle divulgation ne peut être reconnue ou rendue exécutoire qu'en vertu d'un accord international en vigueur entre l'Etat demandeur et la Principauté de Monaco, sans préjudice d'autres motifs de transferts en vertu du présent chapitre.

CHAPITRE IX - COMPETENCE JURIDICTIONNELLE, SANCTIONS PENALES ET DROIT A REPARATION

Article 98

Les tribunaux de la Principauté sont compétents pour connaître de toute action contre un responsable du traitement ou un sous-traitant qui dispose d'un établissement à Monaco dans lequel le traitement en cause a été effectué. Une telle action peut aussi être intentée devant les tribunaux monégasques lorsque la personne concernée a sa résidence habituelle à Monaco, sauf si le responsable du traitement ou le sous-traitant est une autorité publique d'un État agissant dans l'exercice de ses prérogatives de puissance publique.

Lorsqu'un tribunal de la Principauté, compétent pour connaître de la demande, est informé qu'une action concernant le même objet a été intentée à l'égard d'un traitement effectué par le même responsable du traitement ou le même sous-traitant et est pendante devant un tribunal d'un autre État, il contacte cette juridiction pour confirmer l'existence d'une telle action.

Dans le cas prévu à l'alinéa précédent, le tribunal monégasque s'il n'a été saisi en premier lieu peut suspendre l'action introduite devant lui.

Sans préjudice de l'article 12 de la loi n° 1.448 du 28 juin 2017 relative au droit international privé, lorsque cette action est pendante devant des juridictions du premier degré,

le tribunal monégasque peut également se dessaisir, à la demande de l'une des parties, à condition que la juridiction saisie en premier lieu soit compétente pour connaître des actions en question et que le droit applicable permette leur jonction.

Article 99

La personne concernée a le droit de mandater un organisme, une organisation ou une association à but non lucratif, autorisé à Monaco ou reconnu, dont les objectifs statutaires sont d'intérêt public et qui est actif dans le domaine de la protection des droits et libertés des personnes concernées dans le cadre de la protection des données à caractère personnel les concernant, pour qu'il introduise une réclamation auprès de l'Autorité de protection des données en son nom, exerce les recours juridictionnels et exerce en son nom le droit d'obtenir réparation visé à l'article 102.

Article 100

Il est inséré au Livre III, Titre II, Chapitre 1er du Code pénal une section XII intitulée Protection des données personnelles composée de l'article 308-6 rédigé comme suit :

« *Sont punis d'un emprisonnement d'un à six mois et de l'amende prévue au chiffre 3 de l'article 26 du code pénal ou de l'une de ces deux peines seulement :*

1. *ceux qui empêchent ou entravent les investigations opérées pour l'application de la loi ou ne fournissent pas les renseignements ou documents demandés ;*

2. *ceux qui ne tiennent pas un registre des activités de traitements conformément aux dispositions de l'article 26 ;*

3. *ceux qui conservent des données personnelles au-delà de la durée nécessaire à la réalisation des finalités pour lesquelles elles sont traitées ;*

4. *ceux qui, par suite d'imprudences ou de négligences, ne préservent pas ou ne font pas préserver la sécurité des données personnelles au sens de l'article 28 ou divulguent ou laissent divulguer des données personnelles ayant pour effet de porter atteinte à la réputation d'une personne ou à sa vie privée ou familiale ;*

5. *ceux qui méconnaissent les dispositions des articles 22 et 29 ;*

6. *ceux qui transfèrent ou font procéder au transfert de données à caractère personnel en violation des dispositions du Chapitre VIII.*

Sont punis d'un emprisonnement de trois mois à un an et de l'amende prévue au chiffre 4 de l'article 26 du code pénal ou de l'une de ces deux peines seulement :

1. *ceux qui collectent ou font collecter, enregistrent ou font enregistrer, conservent ou font conserver, utilisent ou font utiliser des données à caractère personnel à des fins de surveillance d'une personne à partir d'un système de vidéosurveillance sans avoir obtenu l'autorisation du Ministre d'État prévue à l'article 82 ;*

2. *ceux qui collectent des données à caractère personnel par un moyen frauduleux, déloyal ou illicite ;*

3. *ceux qui à l'occasion de leur traitement, détournent des données à caractère personnel à des fins incompatibles avec les finalités pour lesquelles elles ont été collectées ;*

4. *ceux qui collectent, enregistrent, conservent ou utilisent des données à caractère personnel en dépit de l'opposition des personnes concernées, hors des cas prévus par la loi ;*

5. *ceux qui, à l'exception des autorités compétentes ou des responsables de traitements visés à l'article 77, collectent ou font collecter, enregistrent ou font enregistrer, conservent ou font conserver, utilisent ou font utiliser des données à caractère personnel relatives à la prévention, la recherche, la constatation, la poursuite des infractions pénales ou l'exécution des condamnations pénales ou relatives aux infractions, condamnations, mesures de sûreté ou portant sur des soupçons d'activités illicites ;*

6. *ceux qui, sauf les dérogations prévues par la loi, collectent ou font collecter, enregistrent ou font enregistrer, conservent ou font conserver, utilisent ou font utiliser des données à caractère personnel qui révèlent, directement ou indirectement, des opinions ou des appartenances politiques, raciales ou ethniques, religieuses, philosophiques ou syndicales, ou encore des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique ou des données concernant la santé, la vie sexuelle ou l'orientation sexuelle d'une personne physique.*

En cas de récidive, les peines d'emprisonnement prévues aux deux alinéas précédents ne pourront être inférieures au double de celle précédemment prononcée sans toutefois qu'elles puissent dépasser le double du maximum de la peine encourue. »

Article 101

Toute condamnation prononcée en application de l'article précédent entraîne, de plein droit, la suppression des traitements.

Le Tribunal de première instance peut, en outre, décider la confiscation et la destruction, sans indemnité, des supports des données à caractère personnel incriminées et interdire de procéder à des traitements pendant un délai qui ne peut excéder trois ans ni être inférieur à six mois.

Il peut également ordonner que la personne morale de droit privé soit tenue, solidairement avec son représentant statutaire, au paiement de l'amende prononcée à l'encontre de ce dernier.

L'autorité de protection des données personnelles est rendue destinataire des décisions de justice prononcées en application de l'article 100 ainsi que du présent article.

Article 102

1. Toute personne ayant subi un dommage matériel ou moral du fait d'une violation de la présente loi a le droit d'obtenir du responsable du traitement ou du sous-traitant réparation du préjudice subi.

2. Tout responsable du traitement ayant participé au traitement est responsable du dommage causé par le traitement qui constitue une violation de la présente loi. Un sous-traitant n'est tenu pour responsable du dommage causé par le traitement que s'il n'a pas respecté les obligations prévues par la présente loi qui incombent spécifiquement aux sous-traitants ou qu'il a agi en-dehors des instructions licites du responsable du traitement ou contrairement à celles-ci.

3. Un responsable du traitement ou un sous-traitant est exonéré de responsabilité, au titre du paragraphe 2, s'il prouve que le fait qui a provoqué le dommage ne lui est nullement imputable.

4. Lorsque plusieurs responsables du traitement ou sous-traitants ou lorsque, à la fois, un responsable du traitement et un sous-traitant participent au même traitement et, lorsque, au titre des paragraphes 2 et 3, ils sont responsables d'un dommage causé par le traitement, chacun des responsables du traitement ou des sous-traitants est tenu responsable du dommage dans sa totalité afin de garantir à la personne concernée une réparation effective.

5. Lorsqu'un responsable du traitement ou un sous-traitant a, conformément au paragraphe 4, réparé totalement le dommage subi, il est en droit de réclamer auprès des autres responsables du traitement ou sous-traitants ayant participé au même traitement la part de la réparation correspondant à leur part de responsabilité dans le dommage, conformément aux conditions fixées au paragraphe 2.

CHAPITRE X - DISPOSITIONS FINALES

Article 103

L’autorité de protection des données personnelles succède à la Commission de Contrôle des Informations Nominatives, créée par la loi n° 1.165 du 23 décembre 1993 relative à la protection des informations nominatives, modifiée, en tous ses droits et obligations.

Article 104

Les membres de la Commission de Contrôle des Informations Nominatives en exercice à la date d’entrée en vigueur de la présente loi poursuivent leur mandat en tant que membre de l’autorité de protection jusqu’à la publication de l’ordonnance souveraine procédant à la nomination des membres de ladite autorité.

Article 105

Les responsables du traitement ayant mis en œuvre régulièrement auprès de la commission de contrôle des informations nominatives des traitements de données à caractère personnel avant la date d'entrée en vigueur de la présente loi, et dont l'exploitation se poursuit après son entrée en vigueur, disposent, à compter de cette date, d'un délai d'un an pour mettre leur traitement en conformité avec les dispositions du Chapitre II de la présente loi sous réserve que lesdits traitements n'aient pas été modifiés de manière substantielle.

Les responsables du traitement et les sous-traitants ayant mis en œuvre régulièrement auprès de la commission de contrôle des informations nominatives des traitements de données à caractère personnel avant la date d'entrée en vigueur de la présente loi, et dont l'exploitation se poursuit après son entrée en vigueur, disposent, à compter de cette date, d'un délai d'un an pour se mettre en conformité avec les obligations prévues aux articles 26, 27 et 28, 4ème alinéa, du Chapitre IV. Ce délai est porté à 3 ans pour les responsables du traitement afin de procéder à l'analyse d'impact prévue à l'article 32 au titre de la réévaluation des risques.

Les responsables du traitement dont les traitements de données à caractère personnel relèvent de l'article 61 disposent, à compter de l'entrée en vigueur de la présente loi, d'un délai de cinq ans pour mettre leurs traitements en conformité avec les dispositions des articles 66 et 67. Ce délai n'est pas applicable aux traitements déjà soumis à l'obligation de journalisation.

Article 106

Lorsque des formalités préalables à la mise en œuvre des traitements, initiées sous l'empire de la loi n° 1.165 du 23 décembre 1993, modifiée, précitée, sont en cours d'instruction auprès de l'autorité de protection, celle-ci informe les responsables du traitement de la nature de leurs nouvelles obligations.

Article 107

La liste des traitements inscrits au répertoire institué par l'article 10 de la loi n°1.165 du 23 décembre 1993, modifiée, précitée, est mise à la disposition du public par l'autorité de protection des données personnelles pendant une durée de 10 ans à compter de l'entrée en vigueur de la présente loi.

Article 108

Les recommandations adoptées par la Commission de Contrôle des Informations Nominatives sur le fondement de la loi n° 1.165 du 23 décembre 1993, modifiée, précitée, demeurent en vigueur jusqu'à ce qu'elles soient modifiées, remplacées ou abrogées par l'autorité de protection.

Article 109

A l'article premier de la loi n° 1.444 du 19 décembre 2016 portant diverses mesures en matière de protection des informations nominatives et de confidentialité dans le cadre de l'échange automatique de renseignements en matière fiscale, la référence à l'article 14 de la loi n° 1.165 du 23 décembre 1993, modifiée, précitée, est remplacée par la référence à l'article 10 de la présente loi.

Article 110

A l'article 2 de la loi n° 1.444 du 19 décembre 2016, précitée, la référence aux articles 18 à 19 de la loi n° 1.165 du 23 décembre 1993, modifiée, précitée, est remplacée par la référence aux articles 43 à 47 de la présente loi.

Article 111

Aux articles 24 et 25 de la loi n° 1.362 du 3 août 2009 relative à la lutte contre le blanchiment de capitaux, la référence à l'article 15-1 de la loi n° 1.165 du 23 décembre 1993, modifiée, précitée, est remplacée par la référence à l'article 71 de la présente loi.

A l'article 64-5 de la loi n° 1.362 du 3 août 2009, modifiée, précitée, la référence à l'article 15 de la loi n° 1.165 du 23 décembre 1993, modifiée, précitée, est remplacée par la référence à l'article 11 de la présente loi.

Article 112

Les termes « *informations nominatives* » s'entendent au sens « *données personnelles* » ou de « *données à caractère personnel* » dans les textes législatifs et réglementaires pris avant l'entrée en vigueur de la présente loi.

Article 113

Les modalités d'application de la présente loi sont fixées par ordonnance souveraine.

Article 114

La mention de la présente loi se substitue à celle de la loi n°1.165 du 23 décembre 1993, modifiée, précitée, dans tous les textes législatifs et réglementaires pris avant son entrée en vigueur.

La loi n° 1.165 du 23 décembre 1993 relative à la protection des informations nominatives est abrogée.