

2019-5  
14 mars 2019

## **PROJET DE LOI RELATIVE A L'IDENTITE NUMERIQUE**

### EXPOSE DES MOTIFS

Le début du XXIème siècle est marqué par le développement exponentiel de l'internet et des réseaux sociaux. Le développement des outils technologiques et informatiques crée des bouleversements socio-économiques sans précédent et les frontières du monde réel viennent se confondre avec celles du monde virtuel.

De fait, l'accélération des progrès des technologies numériques n'a de cesse de transformer ces espaces dans lesquels nous vivons et désormais, chaque utilisateur d'internet dispose d'une « *identité numérique* », notion protéiforme constituée des traces qu'il laisse sur la toile savoir notamment, adresses mail, pseudonymes, profils sur les réseaux sociaux ou encore adresses IP.

Aussi, afin que tout un chacun puisse bénéficier de ces réalités contemporaines, il est indispensable de créer et de mettre en œuvre un encadrement juridique qui lui soit propre et qui permette de sécuriser l'accès des personnes aux nouveaux biens et services de manière à assurer la préservation tant de l'information même que de celle des données personnelles échangées.

La réponse la plus appropriée qu'un Etat de droit puisse apporter consiste en la création d'une identité numérique qui s'appuie sur des mécanismes d'authentification performants, permettant d'apporter aux utilisateurs la confiance nécessaire dans l'utilisation de l'outil internet et des réseaux de communication.

Le Gouvernement princier ne fait pas référence ici à l'identité dite « *classique* » des personnes physiques et morales dans le monde réel, concret, que nous connaissons, et qui est caractérisée d'une part, pour les personnes physiques par les éléments constitutifs de l'Etat civil et d'autre part, pour les personnes morales, par les éléments répertoriés au sein du Répertoire du Commerce et de l'Industrie mais bien à un concept différent, une identité spécifique, dite « *numérique* ».

De fait, si l'identité dite « *classique* » est juridiquement encadrée par le droit et les autorités publiques, il en est autrement dans le monde dit « *numérique* » où ce nouveau concept ne dispose actuellement d'aucun type d'encadrement.

Or, les usages liés à l'identification numérique sont nombreux et nécessitent des données d'identification numériques diverses pouvant prendre la forme de mots de passe ou de noms d'utilisateurs. Ces éléments d'identification, appelés communément « *identifiants* », tels que les codes d'accès, les noms d'utilisateurs ou encore les pseudonymes sont nécessaires pour accéder à des sites, qu'ils soient de e-service ou de e-Commerce ou encore aux réseaux sociaux.

Des pans entiers de l'identité des personnes sont ainsi dispersés et morcelés au sein de diverses plate-formes. Cette nouvelle réalité expose les individus à des risques juridiques d'une gravité sans précédent et l'absence de réglementation entraîne une absence de protection qui expose par là même les personnes qui en font usage à un risque réel d'usurpation de leur identité mais également aux diverses fraudes inhérentes à ces nouveaux usages sur les réseaux numériques.

A titre d'exemple, l'identité usurpée peut permettre à des personnes mal intentionnées de commettre des infractions sous couvert de l'identité d'une autre personne et à son entier préjudice.

Dans ce contexte, la nécessité de pouvoir justifier de son identité via des processus fiables permettant l'identification et l'authentification des personnes ainsi que leur encadrement juridique est devenu un impératif.

Le pas a été franchi par un certain nombre d'Etats étrangers. Parmi eux peuvent utilement être cités :

L'Union européenne qui a adopté le règlement (UE) n° 910/2014 du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (eIDAS) (JOUE du 28 août 2014, L. 257/73), lequel définit l'identification numérique en son article 3.1 et élabore, en son article 6, la reconnaissance mutuelle et l'interopérabilité des schémas d'identification électronique lorsqu'elle est notifiée par un Etat membre à la Commission et publiée au Journal Officiel de l'Union européenne. Ainsi, un citoyen d'un Etat membre disposant d'un moyen d'identification d'un niveau de garantie adéquat pour accéder à un téléservice d'un autre Etat membre pourra ainsi en bénéficier sans démarche particulière et ce depuis le 29 septembre 2018. Au surplus, le règlement eIDAS laisse la possibilité aux Etats membres de faire en sorte que les moyens d'identification soient utilisés non seulement dans le secteur public, mais également dans le secteur privé.

De son côté, L'Estonie, a mis en œuvre le principe de citoyenneté numérique dès l'an 2000 avec sa loi n° RT I 2000, 26, 150 du 8 mars 2000 sur la signature électronique. Cette citoyenneté numérique estonienne repose sur l'attribution d'un identifiant unique aux personnes concernées afin de réaliser des démarches administratives et des services d'administration électronique ou « *e-Services* ». Ces téléservices sont aussi divers que variés et concernent le domaine de la santé publique, ou bien des domaines touchant à la vie politique du pays comme le vote électronique.

Au surplus, afin d'attirer des investisseurs étrangers, l'Etat Estonien a aussi mis en place le statut de « *e-résident* » permettant à des personnes physiques ou morales non-résidentes de créer un compte en banque ou encore de créer une entreprise sur Internet via une procédure en ligne simplifiée.

L'Allemagne dispose, quant à elle, de nombreux textes relatifs à l'identité électronique tels que la loi « *Personalausweisgesetz [PAuswG]* » du 18 juin 2009 et l'ordonnance « *Personalausweisgesetz [PAuswV]* » du 1er novembre 2011 relatives à la carte d'identité électronique et l'identité électronique. A côté des institutions, d'autres projets privés ont abouti ou en sont sur le point comme « *Verimi* » qui allie plusieurs groupes de différents secteurs d'activité (banques, industriels, opérateurs télécoms, ...). Ce service, encore en phase de test, permet à une personne de se voir attribuer un identifiant numérique unique permettant d'accéder aux services en ligne proposés par les membres de « *Verimi* ».

L'Italie a, avec un règlement de l'Agence nationale pour le numérique en date du 24 octobre 2014, mis en place le Système Public d'Identité Numérique (« *SPID* »), qui constitue la solution permettant aux citoyens italiens d'accéder à tous les services en ligne de l'administration publique grâce à un identifiant unique (nom d'utilisateur et mot de passe) utilisable à partir d'ordinateurs, de tablettes et de smartphones. Cet identifiant unique peut être créé et attribué par le service fournisseur d'identité choisi par la personne et assurera également son authentification.

De son côté, la Grande Bretagne dispose d'un service d'identité privé en ligne dénommé « *Verify* », qui permet, entre autres, de régler ses impôts en ligne, de signer électroniquement des documents et d'accéder à d'autres téléservices. Ce service est accessible à l'ensemble des résidents du Royaume Unis donc également aux non citoyens de l'Etat.

Enfin, en ce qui concerne le pays voisin, il dispose, s'agissant des téléservices publics, du système « *France Connect* » depuis juillet 2015. Ce téléservice ne regroupe aujourd'hui que des téléservices publics mais pourrait à l'avenir être ouvert aux services offerts par des personnes privées. En effet, La France a, dans sa loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, ouvert l'identité numérique au secteur privé. Ainsi, l'article L. 102-I du Code des postes et communication électroniques qui reprend la définition de l'identification électronique du règlement eIDAS permet, si le moyen d'identification est considéré comme fiable par l'agence nationale de la sécurité des systèmes d'information (A.N.S.S.I.), de l'utiliser dans le cadre de téléservices privés.

Sur le plan international, de nombreux autres Etats disposent également de textes juridiques en matière d'identité électronique savoir notamment :

Aux Etats-Unis, l'Etat de Virginie dispose, dans le chapitre 50 du Code de Virginie, d'une loi sur la gestion de l'identité électronique, le « *Virginia electronic identity management act* » (VA House Bill 1562/Senate Bill 814) du 23 mars 2015 qui établit notamment un régime de responsabilité des opérateurs du cadre de confiance de l'identité. L'Etat du Vermont a créé, lui, par sa récente loi n° 205-2018 du 31 mai 2018 un nouveau type d'entité commerciale spécialisée qui permet à des entreprises de gérer des données personnelles, c'est-à-dire de communiquer non seulement des éléments de données à caractère personnel, mais aussi de fournir des services de certification

Le Benin, avec la loi n° 2017-20 du 13 juin 2017 portant code du numérique en république du Benin encadre notamment, en son article 281, la responsabilité des gestionnaires de systèmes d'identification.

Enfin, la Commission des Nations Unies pour le droit commercial international (CNUDCI) a lancé en 2012 des travaux juridiques sur la gestion d'identité et sur les services de confiance en s'inspirant de ce qui a été déjà réalisé au niveau de l'Union européenne et de certains Etats. Ces travaux sont publiés notamment dans le dernier rapport du groupe de travail n°4 sur le Commerce électronique dans le cadre des travaux de sa cinquante-sixième session (New York, 16-20 avril 2018, doc. A/CN.9/936 du 27 avril 2018 ([www.uncitral.un.org](http://www.uncitral.un.org))).

Face à ces nouveaux défis, le Gouvernement princier souhaite inscrire la Principauté dans une ère de modernité en mettant en place un cadre juridique approprié permettant de poursuivre cinq objectifs principaux :

- répondre aux problématiques existantes et à venir relatives à l'identité numérique aux moyens de dispositions suffisamment générales, permettant des évolutions futures ;
- la création et l'attribution d'une identité numérique monégasque représentant une personne physique ou morale de manière univoque ;
- la création d'un registre national monégasque aux fins notamment de centraliser et de sécuriser les données ;
- sécuriser l'identité numérique, les moyens d'identification numériques et les données d'identification personnelle pour éviter tout type de fraude ;
- instaurer la reconnaissance de cette identité par les plate-formes de service de confiance.

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 articles définissant d'une part, les termes utilisés dans le domaine de l'identité numérique et créant d'autre part, le cadre juridique nécessaire pour la mise en place de ladite identité.

L'article premier du projet de loi a pour objectif de définir les termes importants utilisés communément dans le monde du numérique et ce, dans un souci de précision et de contextualisation. Sont ainsi définis, la notion d'identification numérique qui est entendue comme un processus consistant à utiliser des données d'identification personnelles sous une forme électronique numérique permettant de représenter de manière univoque une personne physique ou morale ; la notion de données d'identification personnelles, définies quant à elles, en prenant en compte l'ensemble des données utilisées dans le processus d'identification, savoir notamment les caractéristiques de la personne telles que le nom, le prénom, les données biométriques ou autres.

Dans le même sens, les données biométriques sont définies comme des caractéristiques physiques ou physiologiques inhérentes à la personne comme les empreintes digitales, ou les données ADN d'une personne physique. Elles se différencient des noms, prénom, date de naissance qui sont des caractéristiques déclaratives de l'identité de la personne en ce sens qu'elles sont inhérentes à la personne physique.

Une fois que l'on a attribué une identité numérique, il faut être en mesure d'authentifier la personne qui se dit en être titulaire, c'est ici qu'intervient le processus d'authentification qui est ainsi défini comme le processus de vérification de l'identité d'une personne mis en œuvre par le fournisseur d'identité aux fins de s'assurer que la personne à qui elle délivre le moyen d'identification est celle qu'elle prétend être.

S'agissant ensuite des moyens d'identification numérique, la définition vise le support de l'identité. Qu'il soit matériel, à l'instar notamment des cartes et flashs codes, ou immatériel comme notamment l'identifiant numérique unique de la personne stocké dans le Registre national monégasque.

Afin de décliner l'ensemble des composants de l'identité numérique, le projet de loi définit opportunément les notions d'identifiant numérique, de fournisseur d'identité et de service de confiance. De fait, l'identifiant, est attribué aux personnes physiques ou morales qu'elles soient monégasques ou non, résidentes, employées à Monaco ou encore touristes.

Différents fournisseurs d'identité pourront créer et attribuer un identifiant numérique sur des supports divers liés à la même identité numérique, donc désignant une même personne. Les fournisseurs d'identité sont entendus, au sens du projet de loi, comme les personnes physiques ou morales qui mettent en œuvre, assurent la maintenance et gèrent les données d'identification qui correspondent aux moyens d'identification. Ils sont responsables de l'identité des personnes. Cette définition permet de préciser la responsabilité des différents acteurs dans le processus d'élaboration, de maintenance et de gestion des données d'identification correspondant aux moyens d'identification.



Enfin, les services de confiance sont quant à eux définis comme des services électroniques fournis à titre onéreux ou non. Les services fournis à titre onéreux peuvent être l'envoi de courriers recommandés électroniques ou encore la signature électronique d'un acte juridique (ex : un contrat) et les services de confiance fournis à titre gratuit peuvent être notamment la réalisation de formalités administratives en ligne via des téléservices.

L'article 2 vient caractériser les éléments qui permettent d'établir les principes essentiels de l'identité numérique d'une personne.

De fait, le premier alinéa de l'article 2 définit spécifiquement ce qu'est l'identité numérique en ce qu'elle est constituée de données d'identification personnelle sous une forme électronique.

Il est en effet apparu hautement opportun au Gouvernement de consacrer le principe de l'identité régaliennne. Le fondement d'une telle démarche réside dans le fait que, sans mise en place d'un véritable cadre de référence de l'identité numérique, la confiance numérique peut rester une notion totalement abstraite et par là même, entraîner une défiance vis-à-vis de l'utilisation des services en ligne. Au surplus, deux finalités gouvernent l'identité régaliennne, une finalité de police permettant aux personnes identifiées de prouver leur identité aux services publics compétents et une finalité de e-service permettant l'utilisation des services de confiance régaliens afin d'accomplir des formalités administratives. Grâce à l'identité numérique régaliennne, ces deux finalités sont sécurisées et leur complémentarité améliorée. Elle sera donc créée et attribuée par les services de l'Etat, mais son utilisation pourra être plus large.

Les deuxième et troisième alinéas précisent, quant à eux, comment sont établies l'identification et l'authentification des personnes physiques.

En effet, l'identité numérique repose sur des données d'identification strictement personnelles et sensibles qui ne doivent en aucun cas être falsifiées. A cette fin, la création et l'attribution de l'identité numérique supposent un niveau élevé de sécurité. Dans cette optique, la création et l'attribution de l'identité numérique devront être à jour des normes de sécurité européennes les plus performantes et des cas d'usages mis en œuvre en Europe. Elle dépendra par ailleurs d'un schéma d'identification qui lui est propre.

Force est de constater que l'identité numérique sera utilisée de manière très fréquente en raison de la multiplication et de la facilité d'utilisation des services électroniques dont des services de confiance. De fait, une personne identifiée numériquement pourra avoir besoin de justifier son identité pour réaliser des formalités administratives, ou encore pour accomplir une transaction électronique plusieurs fois par jour. Cette fréquence d'utilisation entraîne l'élévation du niveau d'exigence en matière de sécurité qui, pour les relations entre les services exécutifs de l'Etat et les administrés, relève du référentiel Général de Sécurité annexé à l'arrêté ministériel n° 2017-835 du 29 novembre 2017 portant application de l'article 54 de l'Ordonnance Souveraine n° 3.413 du 29 août 2011 portant diverses mesures relatives à la relation entre l'Administration et l'administré, modifiée.

Après réflexion, et pour des raisons stratégiques, le Gouvernement princier a fait le choix, au sein de l'article 3, de ne créer et attribuer une identité numérique qu'à deux catégories de personnes. D'une part, les personnes de nationalité monégasque, inscrites sur le sommier de la nationalité monégasque selon les modalités de l'Ordonnance Souveraine n° 2.194 du 12 mai 2009 relative au Sommier de la nationalité monégasque et d'autre part, les personnes titulaires d'un titre de séjour dans les conditions fixées par l'ordonnance souveraine n° 3.153 du 19 mars 1964 relative aux conditions d'entrée et de séjour des étrangers dans la Principauté.

En effet, le plus haut niveau de sécurité qui entourera la délivrance de l'identité numérique n'apparaît pas nécessaire en ce qui concerne la majorité des services numériques.

Pour ce qui en est des autres catégories de personnes, qu'elles soient physiques ou morales, le Gouvernement a entendu ne créer et n'attribuer qu'un identifiant numérique, selon les conditions décrites à l'article 4, à toute personne physique ou morale inscrite dans un registre d'un service exécutif de l'Etat ou d'un service de la commune, tenu en vertu d'une disposition légale ou réglementaire.

Concrètement, un identifiant numérique pourra être attribué aux personnes bénéficiant, par exemple, de prestations médicales de l'Etat en vertu de l'arrêté ministériel du 4 février 1947 portant règlement des prestations médicales, chirurgicales et pharmaceutiques allouées aux fonctionnaires, ou encore des personnes bénéficiant d'un abonnement aux services des parking publics de la Principauté.

L'introduction des personnes morales, au sein de cet article permet de leur attribuer également un identifiant numérique, lequel leur permettra de s'inscrire dans les pratiques européennes et prendre part au marché unique numérique ainsi que de participer à des marchés publics en ligne.

Dans le but d'élargir le spectre des acteurs et des personnes concernées, le deuxième alinéa de l'article 4 autorise les personnes relevant du secteur privé à créer et attribuer des identifiants numériques. Ainsi, des personnes bénéficiant de soins de santé ou de prestations diverses telles que, à titre d'exemple, les touristes, pourront se voir attribuer un identifiant numérique. Cet identifiant numérique se matérialisant sous la forme d'un « pass » pourra être, tel que le prévoit l'article 9 du présent projet de loi, centralisé dans le Registre national monégasque.

Un identifiant numérique pourra également être attribué à des personnes physiques ou morales relevant du secteur privé comme cela pourra être le cas pour les personnes titulaires d'un permis de travail en Principauté.

L'identifiant numérique constitue également un moyen d'accéder à des services délivrés par des plate-formes électroniques. C'est pourquoi, celui-ci devra respecter le niveau de garantie déterminé par le schéma d'identification électronique dont il dépend. Les spécifications des niveaux de garantie faible, substantiel et/ou élevé sont déterminées en fonction du Référentiel Général de Sécurité, précité.

Ainsi, l'identifiant numérique dépend du degré accordé à l'identité revendiquée ou prétendue d'une personne en terme de fiabilité, et est caractérisé sur la base de spécifications techniques, de normes et procédures y afférent, y compris les contrôles techniques dont l'objectif est de réduire et d'empêcher l'utilisation abusive ou l'altération de l'identité.

Les spécifications des identifiants numériques ainsi que leurs niveaux de garantie sont précisés par ordonnance souveraine.

Afin de donner toute son effectivité à l'identification numérique, le Gouvernement a voulu créer avec les articles 5 et 6, un Registre national monégasque. Ce registre a notamment pour vocation de centraliser les identités des personnes disposant d'un identifiant numérique dans le but, d'une part d'assurer l'identification des personnes physiques ou morales et d'autre part, de participer à la réalisation de documents d'identité et par là même, de participer à la lutte contre la fraude (article 5).

Le Registre national monégasque a également pour finalité de mettre à disposition des responsables de fichiers des services publics, des données de personnes physiques ou morales dans les limites des pouvoirs qui leurs sont légalement conférés, et par là même de simplifier les formalités administratives exigées par les autorités publiques.

La centralisation de ces données au sein dudit Registre permettra notamment de préserver l'historique de ces données ou que lesdites données soient anonymisées à des fins statistiques (article 6).

De fait, ce registre aura vocation à améliorer l'efficacité des services électroniques de l'Etat et de la Mairie de Monaco et son utilisation se fera dans le strict respect de la loi n° 1 165 du 23 décembre 1993 relative à la protection des informations nominatives, modifiée.

Il importe au Gouvernement de préciser que le Registre national bénéficiera d'un haut niveau de sécurité en terme de disponibilité, d'intégrité, de confidentialité et de traçabilité et qu'il ne pourra, en aucune façon, remplir des fonctionnalités de fichage et de traçage des personnes physiques ou morales.

Dans un but de protection des données personnelles, aucune interconnexion entre l'identité numérique et les données d'identification personnelle émanant de différents services de l'Etat et qui comprennent les attributs inhérents à la personne ne pourront être effectués.

Au surplus, l'utilisation du Registre national ne pourra servir à déterminer les opinions, les appartenances politiques, raciales, ethniques, religieuses, philosophiques ou syndicales, ni à obtenir les données relatives à la santé, aux particularités génétiques, à la vie sexuelle, aux mœurs, et aux mesures à caractère social.

En pratique, sur le plan technique, un cloisonnement des différentes informations caractérisant l'individu est réalisé. A titre d'exemple, la Sûreté publique ne pourra en aucun cas avoir accès aux données de santé d'une personne qui ne seront accessibles que par les autorités compétentes et ces dernières ne pourront accéder au casier judiciaire de cette personne.

Les modalités d'application des articles 5 et 6 sont précisées par ordonnance souveraine.

L'article 7 prévoit l'élaboration et la mise en œuvre d'une plateforme de services dans le but d'offrir un certain nombre de services délivrés par l'Etat. Ces services peuvent ou non être qualifiés de services de confiance. Lorsque la plate-forme délivre des services de confiance, ils peuvent être fournis à titre gratuit ou à titre onéreux. Ces services de confiance consistent en une identification ou une authentification numérique.

Ainsi, pourront être qualifiées de plate-formes de services toutes celles qui jouent le rôle d'intermédiaire électronique entre la personne titulaire d'une identité numérique (ou d'un identifiant) et la réalisation d'un service de confiance ou non.

Lesdites plate-formes permettent à leurs utilisateurs de bénéficier de services divers comme, envoyer un envoi recommandé électronique via les services postaux, réaliser la signature électronique de documents, bénéficier d'une datation électronique pour un acte juridique ou pour la réalisation d'une action.

Au surplus, les plate-formes de services peuvent également être des fournisseurs d'identité lorsqu'elles émettent des moyens d'identification électroniques et gèrent la procédure d'authentification pour bénéficier des services électroniques qu'elles délivrent.

L'article 8 décrit les missions du fournisseur d'identité et affirme le principe général de sa responsabilité aux fins de protéger la partie utilisatrice des conséquences du détournement de son identité.

Cette responsabilité en termes de délivrance d'un moyen d'identification et de gestion de la procédure d'authentification est rattachée par le biais du quatrième alinéa au régime de droit commun de la responsabilité civile, pénale et administrative.

Les modalités du présent article sont fixées par ordonnance souveraine.

La possibilité d'accéder et de bénéficier des plate-formes de services et d'administration électronique est donc réalisée selon les dispositions de l'article 9, grâce à l'attribution, par un fournisseur d'identité, qu'il soit étatique ou non, d'identifiants permanents ou temporaires à une personne physique ou morale.

Il importe au Gouvernement de relever que la durée de vie des identifiants sera attachée à la durée du service fourni par la plate-forme de service et d'administration électronique. Elle peut donc être permanente ou temporaire selon les utilisations.

Ainsi, à titre d'exemple, un identifiant numérique permanent créé et attribué à une personne pourra notamment permettre de réaliser des formalités administratives pour être conforme aux obligations qui leur incombent via un compte personnel, ou encore de réaliser des formalités déclaratives afin de créer une entreprise.

Un identifiant numérique temporaire pourra, lui, être créé et attribué par des plate-formes de services et d'administration électronique qui délivrent des services sporadiques à des personnes déterminées notamment en matière touristique car ne disposant pas d'une identité numérique régaliennne.

La précision apportée par le deuxième alinéa relatif à la délivrance sur tous types de supports électroniques ou non inscrit la loi dans la perspective du futur et permet de couvrir les innovations technologiques à venir.

Les identifiants numériques seront tous centralisés dans le Registre national monégasque pour en assurer une gestion et une sécurité optimales.

Les modalités d'application de cet article sont précisées dans une ordonnance souveraine.

Enfin, pour assurer la cohérence des textes législatifs et réglementaires préexistants, l'article 10 établit une équivalence sémantique entre les termes « électronique » et « numérique » lorsqu'ils sont utilisés en matière d'identité et de services de confiance. Cette équivalence ne concerne que les lois et règlements en matière d'identité et de services de confiance.

Tel est l'objet du présent projet de loi.



## PROJET DE LOI

### Article premier

Au sens de la présente loi, on entend par :

- « *Identification numérique* » : processus consistant à utiliser des données d'identification personnelle sous une forme électronique représentant de manière univoque une personne physique ou morale, ou une personne physique représentant une personne morale ;
- « *Données d'identification personnelle* » : un ensemble d'informations permettant d'établir l'identité d'une personne physique ou morale, ou d'une personne physique représentant une personne morale ;
- « *Authentification* » : un processus électronique qui permet de confirmer l'identification électronique d'une personne physique ou morale ;
- « *Moyen d'identification numérique* » : un élément matériel et ou immatériel contenant des données d'identification personnelles et utilisées pour s'authentifier pour un service en ligne ;
- « *Identifiant numérique* » : combinaison de lettres, de chiffres ou de symboles fournis par les autorités compétentes qui, considérés isolément ou non, permettent de représenter une personne physique ou morale de manière univoque ;
- « *Données biométriques* » : 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 ;
- « *Fournisseur d'identité* » : une personne physique ou morale responsable de l'identification des personnes physiques ou morales, chargée de l'émission des moyens d'identification électronique ainsi que de la maintenance et la gestion (du cycle de vie) des données d'identification correspondant auxdits moyens d'identification.
- « *Service de confiance* » : un service électronique fourni à titre onéreux ou non qui consiste notamment : en une identité, une authentification, une signature, un cachet, de l'horodatage, une authentification de site internet, ainsi que des certificats relatifs à ces services.

## Article 2

L'identité numérique d'une personne est constituée de données d'identification personnelle sous une forme électronique représentant de manière univoque une personne physique ou une personne physique représentant une personne morale.

L'identification des personnes physiques est établie notamment sur la base de données biométriques transformées en données numériques.

L'authentification des personnes physiques sera réalisée sur la base des éléments relatifs à l'identité numérique de ces dernières.

## Article 3

Une identité numérique est créée et est attribuée :

1°) à toute personne physique inscrite sur le sommier de la nationalité monégasque ;

2°) à toute personne physique titulaire d'un titre de séjour dans les conditions fixées par l'Ordonnance Souveraine n° 3.153 du 19 mars 1964 relative aux conditions d'entrée et de séjour des étrangers dans la Principauté ;

Les modalités d'applications du présent article sont fixées par ordonnance souveraine.

## Article 4

Un identifiant numérique est créé et attribué à toute personne physique ou morale enregistrée dans un registre d'un service exécutif de l'Etat ou d'un service de la commune, tenu en vertu d'une disposition législative ou réglementaire dont la liste est publiée par ordonnance souveraine.

Nonobstant les dispositions du premier alinéa, un identifiant numérique peut être créé et attribué à des personnes physiques ou morales par des personnes relevant du secteur privé.

Les spécifications de l'identifiant numérique sont déterminées en fonction des niveaux de garantie faible, substantiel et élevé fixés par ordonnance souveraine.

Les modalités d'application du présent article sont fixées par ordonnance souveraine.

### Article 5

Il est créé un registre national monégasque qui a pour finalités :

- l'identification des personnes physiques et morales avec l'attribution d'un identifiant numérique ;
- la participation à la réalisation des documents d'identité ou d'autres documents permettant d'établir celle-ci ;
- la participation à la prévention et à la lutte contre la fraude à l'identité.

Le registre national monégasque garantit l'exactitude des données enregistrées sur la base de pièces justificatives. Toute autre donnée y sera traitée comme donnée purement informative.

Les modalités d'applications du présent article sont fixées par ordonnance souveraine.

### Article 6

Le registre national monégasque a également pour finalités :

- la mise à disposition de données de personnes physiques ou morales aux responsables des fichiers des services publics dans les limites des missions qui leur sont légalement conférées aux fins de faciliter l'échange d'information entre lesdits services ;
- la préservation de l'historique de ces données à des fins administratives ou, à condition que les données soient anonymisées, à des fins statistiques ;
- la simplification des formalités administratives exigées par les autorités publiques.

Les modalités d'applications du présent article sont fixées par ordonnance souveraine.

### Article 7

Une plate-forme de services peut délivrer un ou plusieurs services de confiance électroniques, fournis à titre onéreux ou à titre gratuit, qui consistent notamment :

- a) en une identification numérique ou une authentification ;

b) en la création, en la vérification et en la validation de signatures électroniques, de cachets électroniques ou d'horodatages électroniques, de services d'envoi recommandé électronique et de certificats relatifs à ces services ; ou

c) en la création, en la vérification et en la validation de certificats pour l'authentification de site internet ; ou

d) en la conservation de signatures électroniques, de cachets électroniques ou des certificats relatifs à ces services.

Ladite plate-forme peut également délivrer d'autres services ou équipements de sécurité reposant sur toute forme de support.

Les modalités d'application du présent article sont fixées par ordonnance souveraine.

### Article 8

Un fournisseur d'identité délivre le moyen d'identification en garantissant l'identité des utilisateurs et gère la procédure d'authentification.

Lorsqu'il délivre le moyen d'identification, le fournisseur d'identité est responsable du dommage causé intentionnellement ou par négligence à toute personne physique ou morale en raison d'un manquement aux obligations qui lui incombent.

Lorsqu'il gère la procédure d'authentification, le fournisseur d'identité est responsable du dommage causé intentionnellement ou par négligence à toute personne physique ou morale pour ne pas avoir assuré la gestion correcte de ce service.

Les deux précédents alinéas s'appliquent dans le respect des dispositions législatives et réglementaires en matière de responsabilité.

Les modalités d'application du présent article sont fixées par ordonnance souveraine.

### Article 9

L'attribution par un fournisseur d'identité d'identifiants numériques permanents ou temporaires, permet à une personne physique ou morale d'accéder à des plates-formes de services et d'administration électronique.

Les identifiants numériques peuvent être délivrés sur tous types de supports, électroniques ou non.

Ils sont centralisés dans le Registre national monégasque.

Les modalités d'application du présent article sont fixées par ordonnance souveraine

#### Article 10

Lorsque les termes « *électronique* » et « *numérique* » sont utilisés, dans les lois et règlements, en matière d'identité et de services de confiance, ils sont considérés comme ayant un sens équivalent.