

Délibération n° 2025-006 du 9 avril 2025

de l'Autorité de Protection des Données Personnelles portant avis par voie d'auto-saisine sur le projet de Loi n° 1093 portant modification de diverses dispositions en matière de numérique

Vu la Constitution du 17 décembre 1962 ;

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

Vu la Convention n° 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et son Protocole additionnel ;

Vu la Loi n° 1.383 du 2 août 2011 pour une Principauté numérique, modifiée ;

Vu la Loi n° 1.483 du 17 décembre 2019 relative à l'identité numérique ;

Vu la Loi n° 1.435 du 8 novembre 2016 relative à la lutte contre la criminalité technologique ;

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

Vu l'Ordonnance Souveraine n° 3.413 du 29 août 2011 portant diverses mesures relatives à la relation entre l'Administration et l'administré, modifiée ;

Vu l'Ordonnance Souveraine n° 8.099 du 16 juin 2020 fixant les conditions d'application de la Loi n° 1.383 du 2 août 2011 pour une Principauté numérique, modifiée, relative aux services de confiance ;

Vu le Règlement (UE) 2024/1183 du Parlement européen et du Conseil du 11 avril 2024 modifiant le règlement (UE) n° 910/2014 en ce qui concerne l'établissement du cadre européen relatif à une identité numérique ;

Vu la délibération n° 2019-120 du 18 septembre 2019 de la Commission de Contrôle des Informations Nominatives portant avis sur la consultation du Ministre d'Etat portant sur le projet de Loi relative à l'identité numérique ;

Vu la délibération n° 2019-121 du 18 septembre 2019 de la Commission de Contrôle des Informations Nominatives portant avis sur la consultation du Ministre d'Etat portant sur le projet de Loi relative à l'économie numérique ;

Vu la délibération n° 2021-063 du 2 avril 2021 de la Commission de Contrôle des informations Nominatives portant avis sur la consultation du Ministre d'Etat relative à l'Ordonnance Souveraine portant application de la Loi n° 1.491 du 23 juin 2020 relative aux offres de jetons ;

Vu la délibération n° 2024-071 du 20 mars 2024 de la Commission de Contrôle des Informations Nominatives portant recommandation sur la publication au Journal de Monaco des Ordonnances Souveraines et des Arrêtes Municipaux de mise à la retraite pour invalidité ;

Vu la délibération n° 2024-072 du 20 mars 2024 de la Commission de Contrôle des Informations Nominatives portant recommandation sur l'évolution des dispositions conduisant à publier automatiquement certaines sanctions disciplinaires des personnels du Secteur Public au Journal de Monaco et la mise en œuvre d'un droit à l'oubli ;

Vu le dépôt au Conseil National en date du 22 mai 2024 du projet de Loi n° 1093 portant modification de diverses dispositions en matière de numérique.

L'Autorité de Protection des Données Personnelles,

Préambule

Le projet de Loi n° 1093 portant modification de diverses dispositions en matière de numérique a été déposé au Conseil National par le Gouvernement le 22 mai 2024.

Comme l'indique la page dédiée du Conseil National, « *Le projet de loi portant modification de diverses dispositions en matière de numérique est issu de la proposition de loi n° 255 adoptée par le Conseil National le 7 décembre 2022. Ce texte entend répondre aux évolutions constatées dans le domaine numérique concernant notamment les services de confiance, l'économie et l'identité numériques, ou encore la dématérialisation des services administratifs* ».

Ce projet de texte entend apporter des modifications aux Lois n° 1.383 du 2 août 2011 pour une Principauté numérique et n° 1.483 du 17 décembre 2019 relative à l'identité numérique en s'inspirant « *des avancées européennes en la matière à la suite de la révision du Règlement eIDAS n° 910/2014 du 23 juillet 2014 ainsi que de l'adoption des règlements sur les services numériques et la gouvernance des données* ».

Il entend ainsi introduire la notion de « *portefeuille d'identité numérique* » mais aussi « *compléter diverses dispositions, dont les sanctions en cas de méconnaissance des règles de sécurité des opérateurs d'importance vitale et la dématérialisation des formalités relatives au paiement de timbres fiscaux* ».

Aussi convient-il de rappeler que l'article 2 alinéa 2 de la Loi n° 1.165 du 23 décembre 1993, en vigueur lors du dépôt du texte, disposait que « *la Commission est consultée par le Ministre d'Etat lors de l'élaboration de mesures législatives ou réglementaires relatives à la protection des droits et libertés des personnes à l'égard du traitement des informations nominatives et peut l'être pour toute autre mesure susceptible d'affecter lesdits droits et libertés* ».

La Loi n° 1.565, venue remplacer la Loi n° 1.165, dispose aujourd'hui en son article 38 que « *L'autorité de protection est consultée par le Ministre d'Etat ou par le Secrétaire d'Etat 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* ».

Cette consultation n'a pas eu lieu avant le dépôt du projet de texte, le 22 mai 2024. En conséquence, le Président de la CCIN a informé le Gouvernement que la Commission avait décidé de s'autosaisir sur ce projet de Loi, eu égard à ses implications sur les droits et libertés des personnes concernées, étant précisé que la notion de « *données à caractère personnel* » se retrouve évoquée à 16 reprises au sein dudit projet de Loi.

Entre temps, la Loi n° 1.565 du 3 décembre 2024 relative à la protection des données personnelles est entrée en vigueur, abrogeant la Loi n° 1.165 du 23 décembre 1993, modifiée. C'est ainsi l'Autorité de Protection des Données Personnelles (APDP), qui se substitue désormais à la CCIN, qui rendra un avis, qui sera publié en application des nouvelles dispositions légales.

Pour développer cet avis, il sera fait référence aux avis de la CCIN n° 2019-120 relatif au projet de Loi pour une Principauté numérique et 2019-121 qui concernait le projet de Loi relative à l'identité numérique, ainsi qu'aux textes régissant la matière au sein de l'Union européenne, et principalement le Règlement eIDAS 2.

Enfin, l'APDP relève que le projet de texte a des impacts significatifs, outre l'identité numérique et les services de confiance, sur le régime de l'accès aux documents administratifs, la réutilisation de données publiques, et plus généralement de la circulation de la donnée au sein ou à partir des traitements de l'Administration.

L'avis de l'APDP sera ainsi scindé entre les modifications projetées de la Loi pour une Principauté numérique et celles projetées qui concernent l'identité numérique.

I. Sur la modification de la Loi pour une Principauté numérique

a) Sur la technologie Blockchain

La CCIN avait appelé l'attention tant du Gouvernement que du Conseil National sur le fait que la technologie de type blockchain permet l'utilisation de données personnelles conduisant, selon les choix techniques opérés, à rendre impossible leur suppression.

Ainsi, la Commission avait rappelé au sein de sa Délibération n° 2021-063 du 2 avril 2021 portant avis sur la consultation du Ministre d'Etat relative à l'Ordonnance Souveraine portant application de la Loi n° 1.491 du 23 juin 2020 relative aux offres de jetons « *que rien ne vient expliciter les technologies blockchain utilisées dans les offres de jetons et définies dans la Loi n° 1.383 avec leur utilisation (clé publique, clé privée, smart contracts), ni encadrer les différences entre ICO et STO. Or, cela a des conséquences sur les informations nominatives exploitées (identifiants, données insérées individualisantes) par les responsables de traitement, leur accessibilité (données accessibles au public, données privées), et dès lors leur sécurité (comment restreindre l'utilisation et l'accessibilité de la donnée en application de la Loi relative à la protection des informations nominatives, ou du Règlement Général sur la Protection des Données pour les acteurs qui y seront soumis ?). A cet égard, la Commission constate que même la définition du jeton ne vient pas définir qu'il permet de remonter directement ou indirectement à son propriétaire* ».

Il lui avait toutefois été répondu que toute saisine en la matière de la CCIN pour avis, notamment lors des modifications de la Loi n° 1.383 précitée, était inutile car cela ne concernait pas les données personnelles.

Aussi, il convient d'attirer l'attention sur les rappels de la CNIL en ce qui concerne ce type de technologie, notamment sur sa page dédiée qui indique que « *Si tous les projets de Blockchain n'impliquent pas de traitement de données à caractère personnel, en pratique, de nombreuses utilisations de cette technologie nécessitent la manipulation de ces données, tant au niveau du contenu que des informations liées aux participants.*

En effet, une Blockchain peut contenir deux catégories de données à caractère personnel :

- *l'identifiant des participants et des mineurs : chaque participant/mineur dispose d'une clé publique, ce qui permet d'assurer l'identification de l'émetteur et du destinataire d'une transaction ;*
- *des données complémentaires, inscrites « dans » une transaction (ex : diplôme, titre de propriété). Si ces données sont relatives à des personnes physiques, éventuellement autres que les participants, directement ou indirectement identifiables, il s'agit de données à caractère personnel.*

Sur la base de cette distinction, la grille d'analyse habituelle du RGPD s'applique : identification du responsable de traitement, mise en œuvre des droits, mise en place de garanties appropriées, obligation de sécurité, etc. ».

Il y est précisé en outre « Les enjeux que présentent la Blockchain en termes de respect des droits et libertés fondamentaux appellent nécessairement une réponse au niveau européen. La CNIL est l'une des premières autorités à se saisir officiellement du sujet et va s'inscrire dans une démarche de coopération avec ses homologues européens pour proposer une approche solide et harmonisée ».

« Elle entend également se rapprocher d'autres régulateurs nationaux (AMF, ACPR) afin de poser les bases d'une interrégulation permettant aux acteurs concernés une meilleure lisibilité des diverses réglementations applicables à la Blockchain ».

Pour conclure sur ce point, M. YOUM Heung Youl, Commissaire à l'autorité de protection des données de Corée du Sud, indique dans un encart du dossier thématique de la CNIL relatif à l'identité numérique, que « L'autorité de protection des données de Corée du Sud (PIPC) considère que l'un des sujets principaux concernant les services basés sur la blockchain est l'absence de possibilité de destruction des données. Les personnes ne peuvent plus faire valoir leur droit à l'oubli. Pour résoudre ces questions, la PIPC recommande ainsi aux services utilisant une blockchain de choisir une mise en œuvre qui ne stocke pas de donnée sur la chaîne de blocs elle-même (les données peuvent être stockées hors chaîne ou sur une chaîne latérale).

Par ailleurs, notre réglementation en protection des données a été amendée en juillet 2022 pour reconnaître que les données à caractère personnel sur une chaîne de blocs peuvent être considérées comme détruites lorsqu'il est impossible d'identifier la personne concernée (en utilisant des techniques d'anonymisation).

Enfin, la PIPC entretient une coopération étroite avec le Ministère des sciences et des nouvelles technologies et le Ministère de l'Intérieur et de la Sécurité pour s'assurer que les aspects relatifs à la vie privée sont considérés au sein des systèmes d'identité et d'authentification basés sur une blockchain ».

L'APDP relève, à l'analyse du présent projet de Loi, qu'aucune disposition ne fait le lien entre les technologies soutenues par le texte et la nécessaire protection des données personnelles, que ce soit sur les actifs numériques, les jetons ou les registres électroniques.

b) Sur le metavers et les avatars

La Loi et le projet de Loi définissent les avatars comme représentant « *l'identité numérique de l'utilisateur au sein d'un métavers* », et ce dernier comme étant « *une plateforme persistante et synchrone créant un ou des univers virtuels immersifs proposant des produits et services en ligne à plusieurs utilisateurs simultanément sous formes d'avatars, pouvant notamment s'y déplacer, y interagir socialement et économiquement* ».

L'ambiguïté que la notion d'« *identité numérique* » du métavers créée dans une Loi ayant de forts liens avec celle sur l'identité numérique délivrée par l'Etat est renforcée par l'absence de tout article dédié aux notions d'avatars ou de métavers. L'APDP estime en outre qu'intégrer en droit interne les « *doubles numériques* » de personnes physiques sur une « *plateforme persistante* » devrait s'accompagner d'une réflexion sur leur devenir au décès des utilisateurs.

c) Sur les articles 7, 9 et 10

Le projet de Loi n° 1093 modifie également certains articles du « *Titre IV – De la responsabilité des prestataires techniques* » de la Loi n° 1.383, susmentionnée, notamment pour intégrer en droit monégasque des éléments figurant dans le Règlement (UE) 2022/2065 du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE dit Règlement sur les services numériques (DSA).

L'APDP observe que sont modifiées uniquement les dispositions relatives aux prestataires d'hébergement (« *personnes physiques ou morales qui fournissent un service de communication au public en ligne, à titre exclusif ou non consistant dans le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par un destinataire du service* ») et ceux de simple transport (« *les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne* »).

A cet égard, l'APDP constate que les termes utilisés pour désigner les différents prestataires ne sont pas les mêmes à Monaco que dans les pays voisins et considère que pour une meilleure appréhension du texte par les personnes concernées par les deux côtés de la frontière, il conviendrait d'adopter un champ lexical commun.

En outre, l'Autorité prend acte que le choix a été fait de ne pas intégrer en droit monégasque les prestataires de « *mise en cache* » visés à l'article 5 du DSA. Par ailleurs, l'APDP souligne que les dispositions relatives aux plateformes en ligne, traitées à l'article 34-1 de la Loi n° 1.383, ne sont pas modifiées par le présent projet. Elle constate que cela crée une divergence avec la nouvelle définition de « *plateforme en ligne* » applicable au sein de l'Union européenne.

S'agissant de l'article 7 du projet de Loi, l'APDP relève qu'il s'agit d'une reprise avec quelques modifications de la rédaction présente dans l'ancienne version de la Loi française n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN). Toutefois, l'Autorité s'interroge sur la référence au « *caractère manifestement illicite* » évoqué à l'alinéa 2 s'agissant de la responsabilité pénale de cet acteur et sur la raison de cette spécificité à Monaco.

Par ailleurs, l'Autorité relève que le dernier alinéa de cet article liste les éléments à notifier aux personnes physiques ou morales qui fournissent un service d'hébergement. Elle observe que la rédaction projetée est celle anciennement présente à l'article 6 de la LCEN. Toutefois, elle constate que le deuxième paragraphe de l'article 16 du DSA allège les éléments à communiquer lors de la notification, avec notamment un *quantum* moindre d'informations relatives à l'identité de la personne à l'origine de l'alerte ou encore l'absence de condition de transmission de la copie du message adressé à l'auteur ou à l'éditeur. Ainsi, l'APDP s'interroge sur la prise en compte du principe de minimisation dans la rédaction de ce dernier alinéa et sur l'efficacité des mécanismes mis en place.

L'Autorité constate que les 2 premiers alinéas de l'article 9 du projet de Loi relatif aux prestataires de simple transport sont inspirés de la rédaction actuelle de l'article 6 III A de la LCEN. S'agissant plus spécifiquement du premier alinéa l'APDP relève qu'il prévoit l'information sur l'existence de moyens techniques permettant aux abonnés de restreindre l'accès à certains contenus. Il est indiqué qu'un Arrêté Ministériel précise « *les fonctionnalités minimales et les caractéristiques techniques auxquelles ces moyens répondent, compte tenu de l'activité de ces personnes* ». A cet égard, l'Autorité considère que si une restriction (de type contrôle parental) sans surcoût afin de protéger les mineurs sur Internet est légitime elle pose des questions relatives à la protection des données personnelles qui sont susceptibles d'être traitées. Ainsi, l'APDP s'interroge sur le choix opéré pour le traitement de ces informations (gestion centralisée ou propre à chaque utilisateur qui en garde la maîtrise) et considère que ces précisions devraient figurer dans un texte d'application.

De plus, l'APDP relève que le dernier alinéa est une réécriture du premier paragraphe de l'article 4 du DSA. Néanmoins, elle constate tout d'abord que ce dernier texte énonce des conditions cumulatives alors que la rédaction projetée par Monaco énonce des conditions alternatives. Enfin, il semblerait qu'une erreur matérielle se soit glissée dans la rédaction de la première condition « *soit elles sont à l'origine de la demande de transmission litigieuse* ». En effet, le fournisseur d'accès (simple transport) peut être à l'origine d'une transmission mais pas d'une demande de transmission. Ainsi, il conviendrait de supprimer « *demande* ».

L'article 10 du projet de Loi prévoit d'ajouter trois alinéas à l'actuel article 32 de la Loi n° 1.383. Ces nouveaux alinéas visent à faire concourir les personnes visées aux articles 29 (prestataires d'hébergement), 32 (prestataires de simple transport) et 31-4 (plateformes en ligne) à la lutte contre certaines infractions visées spécifiquement. Pour ce faire ils doivent mettre en place des dispositifs facilement accessibles et visibles permettant à toute personne de porter à leur connaissance les données relatives à ces infractions. Néanmoins, le dernier alinéa ne soumet que les personnes prévues aux articles 29 et 34-1 à une obligation d'informer promptement les Autorités compétentes de toutes activités illicites. De plus, l'APDP constate que le manquement à cette obligation n'est assorti d'aucune sanction et s'interroge sur l'effectivité de la disposition.

Enfin, l'Autorité prend acte que les modifications envisagées par le projet de Loi 1093 pour y intégrer les dispositions du DSA se limitent aux points sus évoqués. Elle constate dès lors que ne sont pas traités des éléments essentiels issus du texte précédemment cité avec notamment les mécanismes d'action des hébergeurs après notification d'un contenu illicite (délais, réponses, etc.), les dispositions relatives aux conditions générales, les rapports sur la transparence, et les dispositions relatives aux injonctions (d'agir contre des contenus illicites ou de fournir des informations) émises par les Autorités judiciaires et administratives, etc.

d) Sur l'attestation électronique attributs

L'article 12 introduit les attestations électroniques d'attributs telles que prévues au sein de eIDAS 2. L'article 38-3 projeté reprend les dispositions de l'article 45 quater du Règlement eIDAS 2, en retirant toutefois toute possibilité de déroger au principe d'interdiction posé.

L'APDP se demande toutefois si, de manière ponctuelle et sur des traitements ciblés, une dérogation ne permettrait pas de collecter moins de données personnelles que par une authentification « classique ».

L'APDP estime en outre qu'il pourrait être opportun de mentionner, au sein de la Loi, que les attestations électroniques d'attributs délivrées par un organisme du secteur public responsable d'une source authentique, délivrent des attestations d'attributs présentant un niveau de fiabilité équivalent à celui des prestataires de services de confiance qualifiés.

e) Sur la publication des actes individuels

La CCIN avait adopté en 2024 deux délibérations portant recommandation, susvisées, concernant pour l'une la publication au Journal de Monaco des Ordonnances Souveraines et des Arrêtes Municipaux de mise à la retraite pour invalidité, et pour l'autre, la publication automatique de certaines sanctions disciplinaires des personnels du Secteur Public au Journal de Monaco. La nature, l'automatisme et la permanence de ces publications portent gravement atteinte aux droits des personnes concernées.

Aussi, en prévoyant que pour certains actes individuels, il soit garanti qu'ils ne puissent être indexés par les moteurs de recherche, il semble que l'article 14 projeté ait pour objectif de répondre aux problématiques soulevées par la CCIN.

L'APDP relève toutefois que les actes individuels concernés sont « *notamment relatifs à l'état et à la nationalité des personnes* ». Bien qu'il y ait l'adverbe « *notamment* », il n'y a aucune indication que la publication des sanctions soit concernée par la nouvelle protection offerte par l'article 14 projeté. En outre, ne sont concernés par le projet de Loi que les actes publiés par Ordonnance Souveraine ; ne sont ainsi pas inclus, par exemple, les actes publiés par Arrêtes Ministériels ou Municipaux. Aussi elle considère qu'il convient d'étendre cette mesure à ces catégories d'actes individuels.

Par ailleurs, l'APDP relève que la non indexation des actes n'enlève pas la possibilité de publier des Ordonnances Souveraines comportant des données de santé, ni le caractère automatique de la publication d'une sanction (pour rappel, la publicité doit être une mesure de sanction autonome).

Il pourrait ainsi paradoxalement s'opérer un retour en arrière concernant les données de santé, le Ministre d'Etat s'étant par courrier daté du 25 juillet 2024, engagé à ne plus mentionner dans les Ordonnances Souveraines le fait que la mise à la retraite soit due à une invalidité. Depuis cette date, cet engagement est respecté. Il serait donc souhaitable que la mesure projetée ne réintroduise pas la possibilité de publier des données de santé. A cet égard, l'APDP appelle l'attention sur la nécessité de désindexer tous les actes individuels portant sur les personnes mises à la retraite pour invalidité, publiés avant le 25 juillet 2024.

f) Sur la gouvernance de la donnée et l'accès aux documents administratifs

A titre liminaire, l'APDP relève que la Loi n° 1.565 ne prévoit pas en son sein de dérogation liée au principe de l'accès du public aux documents administratifs, à l'inverse de l'article 86 « *Traitement et accès du public aux documents officiels* » du RGPD, dont s'inspire la Loi n° 1.565.

Aussi, comme l'avait mentionné en son temps la CCIN, un régime d'accès et de restrictions d'accès à des documents administratifs, pouvant ou non contenir des données personnelles, sur le seul fondement de l'Ordonnance Souveraine n° 3.413, inférieure dans la

hiérarchie des normes à la Loi relative à la protection des données personnelles, est porteur d'insécurité juridique.

L'article 16 projeté introduit donc à un niveau législatif un régime de communication de documents administratifs.

L'exposé des motifs indique que « *L'article 16 permet ainsi à la Principauté de s'inscrire dans le sillon européen du Règlement (UE) 2022/868 du Parlement européen et du conseil du 30 mai 2022 portant sur la gouvernance européenne des données dit « Data Governance Act (DGA) » et d'utiliser le potentiel économique et sociétal inexploité des données du secteur public dans un cadre clair, précis et protecteur s'inscrivant dans le respect de la réglementation en matière de données à caractère personnel* ».

Le DGA encadre la réutilisation de certaines catégories de données protégées du secteur public, à savoir, en application de son article 3 « *Catégories de données* » :

1. « (...) *aux données détenues par des organismes du secteur public, qui sont protégées pour des motifs :*

a) *de confidentialité commerciale, y compris le secret d'affaires, le secret professionnel et le secret d'entreprise ;*

b) *de secret statistique ;*

c) *de protection des droits de propriété intellectuelle de tiers ; ou*

d) *de protection des données à caractère personnel, dans la mesure où de telles données ne relèvent pas du champ d'application de la directive (UE) 2019/1024.*

2. *Le présent chapitre ne s'applique pas :*

a) *aux données détenues par des entreprises publiques ;*

b) *aux données détenues par des radiodiffuseurs de service public et leurs filiales et par d'autres organismes ou leurs filiales pour l'accomplissement d'une mission de radiodiffusion de service public ;*

c) *aux données détenues par des établissements culturels et des établissements d'enseignement ;*

d) *aux données détenues par des organismes du secteur public qui sont protégées pour des raisons de sécurité publique, de défense ou de sécurité nationale ; ou*

e) *aux données dont la fourniture est une activité qui ne relève pas de la mission de service public dévolue aux organismes du secteur public concernés telle qu'elle est définie par la loi ou par d'autres règles contraignantes en vigueur dans l'État membre concerné ou, en l'absence de telles règles, telle qu'elle est définie conformément aux pratiques administratives courantes dans cet État membre, sous réserve que l'objet des missions de service public soit transparent et soumis à réexamen.*

3. *Le présent chapitre est sans préjudice :*

a) *du droit de l'Union, du droit national et des accords internationaux auxquels l'Union ou les États membres sont parties en ce qui concerne la protection des catégories de données visées au paragraphe 1 ; et*

b) *du droit de l'Union et du droit national en matière d'accès aux documents ».*

La réutilisation est quant à elle définie comme « *l'utilisation, par des personnes physiques ou morales, de données détenues par des organismes du secteur public, à des fins commerciales ou non commerciales autres que l'objectif initial de la mission de service public pour lequel les données ont été produites, à l'exception de l'échange de données entre des organismes du secteur public aux seules fins de l'exercice de leur mission de service public* ».

L'APDP relève toutefois que les données du secteur public sont aussi concernées au sein de l'Union européenne par la Directive (UE) 2019/1024 du Parlement européen et du Conseil du 20 juin 2019 « *concernant les données ouvertes et la réutilisation des informations du secteur public (refonte)* ».

La France, en transposant cette Directive, a choisi une large mise à disposition d'informations, en rendant obligatoire la publication d'un certain nombre de documents, notamment ceux pouvant être concernés par le droit d'accès aux documents administratifs (Livre III Titre Ier du Code des relations entre le public et l'administration).

L'APDP constate que le principe de réutilisation de la donnée sous licence et/ou sous condition d'acceptation de l'Administration, telle que projetée à l'article 16, englobe toutes les données, sans distinction de leur qualité et de leur sensibilité (exemple, le DGA concerne des données confidentielles ou concurrentielles).

Aussi, elle s'interroge sur les limites et les conséquences des dispositions de l'article 16 projeté. Ainsi, se posent notamment les questions suivantes :

- l'article 24 de l'Ordonnance Souveraine n° 3.413, susvisée, suffit-il à limiter les communications indues telles que citées par le DGA quand pèse sur le secteur public une obligation de communication de toute information ;
- dès lors, les risques associés ont-ils été étudiés, comme notamment celui d'abaisser le niveau de protection des données personnelles garanti par la Loi n° 1.565 ;
- les conséquences éventuelles de tout soumettre à un régime de licence et/ou d'autorisation ont-elles été anticipées, et est-il possible pour le secteur public de mettre à disposition des informations libres ? y a-t-il une conséquence pour les informations librement accessibles et publiées aujourd'hui sans licence sur les sites de l'Administration ?

Par ailleurs, l'APDP rappelle que la CCIN avait alerté au sein de son rapport d'activité 2023 quant à de nécessaires réflexions visant à modifier le régime du droit d'accès aux documents administratifs, dont une mauvaise utilisation de l'article 24 de l'Ordonnance Souveraine n° 3.413 avait conduit à sanctionner un responsable de traitement du secteur public.

La CCIN avait estimé que l'encadrement par Ordonnance Souveraine de la matière apparaissait insuffisant et qu'une Loi devrait être le véhicule juridique approprié. L'APDP est confortée dans cette analyse à l'aune de la Loi projetée, qui régit l'ensemble des communications et circulations de données publiques, en maintenant les dérogations aux dites communications et le droit d'accès administratif à un échelon inférieur de la hiérarchie des normes.

En ce qui concerne plus précisément le principe de réutilisation des données projeté, l'APDP rappelle que le projet de Loi dispose que « *La réutilisation d'informations publiques comportant des données à caractère personnel est subordonnée au respect des dispositions en vigueur en matière de protection des données à caractère personnel* ».

Ainsi, l'APDP rappelle que la possible réutilisation des données, et donc le texte projeté, ne doit pas être analysée comme une base légale autonome permettant la réutilisation de données personnelles. Il faudra donc que les entités concernées respectent les dispositions de l'article 5 de la Loi n° 1.565 du 3 décembre 2024 relatives à la licéité du traitement et toutes les conditions de transparence et de prévisibilité attachées à l'exploitation de données personnelles pour un traitement ultérieur, comme prévu à l'article 11 du même texte. En tout état de cause, les dispositions envisagées ne doivent pas concourir à altérer les droits et

libertés fondamentaux des personnes concernées tels que protégés par la Loi relative à la protection des données personnelles.

A cet égard, elle estime contraire « *au respect des dispositions en vigueur en matière de protection des données à caractère personnel* » le fait de prévoir que « *Lorsque la réutilisation n'est possible qu'après anonymisation des données à caractère personnel, l'organisme du secteur public détenteur y procède sous réserve que cette opération n'entraîne pas des efforts disproportionnés* ».

Cette dérogation à l'anonymisation, qui en l'état du texte vaut pour tout jeu de données, qu'il soit ou non sensible (comme des données de santé), n'est pas envisageable eu égard à la Loi n° 1.565.

L'APDP estime qu'en fonction de la nature des informations et des critères retenus, l'article 35 de la Loi n° 1.565 pourrait exiger la réalisation d'une analyse d'impact.

L'Autorité saisit cette occasion pour rappeler qu'anonymiser n'est pas occulter le nom et prénom des personnes concernées mais, en fonction de la quantité d'informations disponibles, avoir la certitude que leur association ne permette en aucune façon de ré-identifier ladite personne.

Elle rappelle également que la mise à disposition de données non anonymisées permettrait leur réutilisation, ce qui pourrait avoir des conséquences pour les droits et libertés des personnes concernées, notamment en termes de transparence et d'exercice des droits.

De plus, l'APDP relève que le responsable du portail interministériel veille « *à ce que la mise à disposition des données de référence s'effectue dans le respect des dispositions législatives et réglementaires en vigueur* », étant précisé que ledit portail est organisé « *dans le respect de la réglementation en vigueur en matière de protection des données à caractère personnel et des secrets protégés par la loi* ». Elle rappelle que ledit responsable ne peut être assimilé à une entité de contrôle.

Sur ce point, en France, le droit d'accès administratif et le régime de la réutilisation de données publiques sont encadrés par la Commission d'Accès aux Documents Administratifs, Autorité Administrative Indépendante à laquelle prend part la CNIL. Dans les autres pays européens, ou au Canada outre Atlantique, il existe également des régimes de contrôles indépendants, par les Autorités de protections des données personnelles ou des Autorités dédiées. Or, en Principauté, en cas de contentieux relatif au rejet d'une demande d'accès aux documents administratifs, le Ministre d'Etat est juge et partie dans l'appréciation du refus. La situation n'est donc pas satisfaisante.

Enfin, l'APDP s'interroge sur ses interactions avec le responsable du portail interministériel, lequel devrait être qualifié de responsable du traitement et les problématiques discutées en direct avec l'APDP, surtout au regard des missions qui lui sont confiées.

g) Sur les échanges de données entre organismes du secteur public

L'article 13 projeté entend simplifier les démarches des administrés en s'inspirant des dispositions de la section 4 « *Echanges de données entre administrations* » du Chapitre IV du Titre 1^{er} du Livre 1^{er} du Code des relations entre le public et l'administration.

En Principauté, les échanges d'informations concernent les « *Organismes du secteur public* » qui sont définis au sein de la Loi n° 1.383 comme étant les « *personnes morales de droit public, autorités publiques, organismes de droit privé investis d'une mission d'intérêt général ou concessionnaires d'un service public* ».

Aussi, si l'Arrêté Ministériel d'application de l'article 13 projeté le prévoit, il est possible qu'il y ait des échanges de données entre l'Administration et des organismes privés, dès lors qu'ils sont à l'origine de ces informations ou les détiennent en raison de leurs missions.

Ainsi, en fonction des choix opérés, la Direction de la Sûreté Publique (DSP), dans le cadre de renouvellements de cartes de séjour ou de délivrances de certificats de résidence, pourrait éventuellement demander à la SMEG des relevés détaillés de consommation, ce qui apparaîtrait disproportionné à l'APDP.

En conséquence, elle estime opportun de recentrer les échanges au sein de l'Administration en excluant les acteurs privés de ce dispositif, le secteur public monégasque ayant des spécificités liées aux titres de séjour et aux monopoles que ne connaît pas l'Administration française, dont s'inspirent les textes en projet.

Par ailleurs, et même si cela n'est pas expressément prévu dans les dispositions projetées (à l'inverse des dispositions françaises), l'APDP rappelle qu'elle devra être saisie pour avis sur le ou les projets d'Arrêtés Ministériels d'application.

Son attention est toutefois appelée sur ce que cet ou ces Arrêté(s) Ministériel(s) est/sont censé(s) encadrer, à savoir « *notamment la durée et les modalités de conservation des informations et des données collectées à cette occasion* » et « *La liste des organismes du secteur public qui se procurent directement des informations ou des données auprès des organismes du secteur public en application du présent article ainsi que la liste des informations ou des données ainsi échangées et le fondement juridique sur lequel repose le traitement des procédures mentionnées au premier alinéa du présent article (...)* ».

Il semble que la formulation choisie encadre à la fois le sort des données lors de leur échange, mais aussi lors de l'exploitation de celles-ci par les organismes du secteur public. Or, les modalités d'exploitation, de licéité, et de conservation des données par lesdits organismes préexistent aux échanges d'informations, étant prévues par des dispositions législatives ou réglementaires.

L'APDP relève en outre qu'il est impossible de prédéfinir de manière exacte de quelles données les organismes peuvent avoir besoin, celles-ci étant fonction de la demande de l'utilisateur, étant précisé que seules les données strictement nécessaires à l'exécution de la demande de l'utilisateur doivent être recueillies.

Elle estime donc que seul le sort des données lors des échanges devrait être encadré par le ou les Arrêtés Ministériels, et notamment leur sécurité, la liste des Administrations autorisées à procéder aux échanges, et les catégories de données à collecter ou à exclure.

L'APDP estime que ces échanges pourraient s'inscrire dans une interface de programmation d'application (API) compatible avec le portefeuille numérique pour que leurs utilisateurs puissent vérifier l'accès et les flux relatifs à leurs données personnelles.

II. Sur la modification de la Loi relative à l'identité numérique

A titre liminaire, l'APDP constate que la notion de partie utilisatrice évolue et sera *in fine* définie à la fois au sein de la Loi sur l'identité numérique et de la Loi pour une Principauté numérique. Elle relève toutefois que la définition diffère en fonction du texte.

La modification projetée au sein de la Loi sur l'identité numérique propose une définition conforme à eIDAS 2 : « *Partie utilisatrice* » : *une personne physique ou morale qui se fie à*

une identification électronique, aux portefeuilles d'identité numérique ou à d'autres moyens d'identification électronique, ou à un service de confiance ».

Tandis que la Loi pour une Principauté numérique propose la définition suivante de la « *partie utilisatrice* » : « *une personne physique ou morale ou une personne physique représentant une personne physique ou morale qui se fie à un service de confiance ou à des moyens d'identification électronique fournis conformément à la présente loi* ».

La seconde semble résulter d'une erreur matérielle, le représentant d'une personne physique n'ayant pas à figurer au sein de la présente définition, et les moyens d'identification électronique ne sont pas « *fournis conformément à la présente loi* » mais conformément à la Loi sur l'identité numérique.

Toutefois, l'APDP estime que cela résulte de la complexité du dispositif mis en place, réparti *a minima* sur les deux textes précités qui partagent, dupliquent ou se renvoient sur de nombreuses dispositions (auxquelles peuvent-être ajoutés dans une certaine mesure le Titre IV de l'Ordonnance Souveraine n° 3.413 du 29 août 2011 portant diverses mesures relatives à la relation entre l'Administration et l'administré, l'Ordonnance Souveraine n° 8.696 du 17 juin 2021 relative à la carte d'identité monégasque et l'Ordonnance Souveraine n° 3.153 sur les conditions d'entrée et de séjour des étrangers).

a) Sur l'objectif du portefeuille d'identité numérique et sur l'identité numérique consentie

L'APDP relève que le projet de Loi dont s'agit introduit, à l'instar du Règlement eIDAS 2, la notion de portefeuille d'identité numérique qui est « *un moyen d'identification électronique qui permet à l'utilisateur de stocker, de gérer et de valider en toute sécurité des données d'identification personnelle et des attestations électroniques d'attributs, afin de les fournir aux parties utilisatrices et aux autres utilisateurs des portefeuilles d'identité numérique et de signer au moyen de signatures électroniques qualifiées ou d'apposer des cachets au moyen de cachets électroniques qualifiés* ».

L'article 18-1 projeté dispose qu'« *Il est instauré un portefeuille d'identité numérique pour garantir à toute personne physique ou morale un accès sécurisé, fiable, continu et transfrontalier à des services publics et privés, tout en exerçant un contrôle total sur leurs données* »

L'exposé des motifs du projet de Loi expose que « *Le portefeuille d'identité numérique est un moyen d'identification numérique. Cet instrument permet notamment d'authentifier le portefeuille d'une autre personne et de recevoir et partager des données d'identification et des attestations électroniques d'attributs de manière sécurisée entre deux portefeuilles ; de signer au moyen de signatures électroniques qualifiées et d'apposer des cachets électroniques qualifiés. Les modalités d'application du portefeuille d'identité numérique sont déterminées par ordonnance souveraine. En outre, le portefeuille prend par exemple en charge des protocoles et interfaces communs et il permet l'interopérabilité avec les moyens d'identification monégasques* ».

Il s'infère de ces éléments que le portefeuille numérique a vocation d'une part à être transfrontalier (sous réserve d'un accord avec l'Union européenne), d'autre part à être interopérable avec les moyens d'identification monégasques. L'APDP estime que les moyens d'identification monégasques ne peuvent être que ceux reconnus pour une authentification aux services publics, donc *a priori*, en l'état, avec le moyen d'identification électronique contenu dans la carte d'identité monégasque et la carte de séjour des résidents.

La notion d'interopérabilité et l'article 18-9 projeté sous-entendent la coexistence de deux systèmes distincts. Pourtant, une lecture *a contrario* de l'article 18-10 projeté laisse à penser que les articles 1 et 2 de l'Ordonnance Souveraine n° 8.693 du 17 juin 2021 portant application des articles 4 et 5 de la Loi n° 1.483 du 17 décembre 2019 relative à l'identité numérique s'appliquent au portefeuille, et donc que ce dernier utilise le même moyen d'identification électronique. De plus l'article 18-3 projeté précise que le portefeuille prend en charge des protocoles et interfaces pour « *que l'utilisateur puisse de manière sécurisée être enrôlé grâce aux moyens d'identification numériques associés* ».

Le projet de texte n'indique pas non plus la répartition éventuelle des rôles entre le fournisseur d'identité, qui, aux termes de sa définition, demeure « *un prestataire de service de confiance qualifié ou non qualifié responsable de l'identification des personnes physiques ou morales, chargé 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* », et le fournisseur de portefeuille d'identité numérique.

Aussi l'APDP constate qu'elle ne peut qu'effectuer des conjectures, eu égard à l'absence :

- d'analyse des besoins monégasques en matière d'identité numérique ;
- de scénarios envisagés eu égard à ces besoins et le notamment sur les moyens techniques à développer et à mettre en œuvre ;
- d'analyse de l'impact du projet de Loi sur le droit interne monégasque.

Elle peut toutefois, à l'aune du texte et des avis de la CCIN sur le sujet, formuler certaines observations.

Il convient dans un premier temps de rappeler que l'identité numérique a pour objectif de sécuriser l'identité des personnes concernées dans l'espace numérique en les protégeant de violations de données ou d'usurpation d'identité, dans le cadre d'une utilisation fluide facilitant les démarches en ligne, notamment auprès de l'Administration. Il s'agit donc d'un outil permettant d'accroître la confiance dans la vie et l'économie numérique, objectif légitime auquel l'APDP ne peut que s'associer.

Concernant sa mise en œuvre, son attention est toutefois appelée sur les modalités choisies. Ainsi, l'APDP rappelle que l'identité numérique est obligatoirement attribuée aux monégasques, ainsi qu'aux résidents.

Il est prévu qu'il en soit de même pour certaines populations visées à l'article 5 de la Loi n° 1.483 qui dispose qu'« *Une identité numérique est créée et est attribuée à toute personne physique ou morale enregistrée dans un registre d'un service public, tenu pour l'application d'une disposition législative ou réglementaire dont la liste est publiée par ordonnance souveraine* ».

La CCIN avait pu entrevoir les prémises d'une première utilisation de cet article 5 lors du déploiement du portail pour l'emploi, qui entendait en outre forcer la connexion des demandeurs d'emploi par l'identité numérique.

Dès lors, l'APDP constate un écart entre l'identité numérique obligatoire (à l'activation facultative néanmoins du moyen d'identification) et le portefeuille numérique, qui repose sur la volonté de l'utilisateur d'y adhérer.

Elle estime donc que le caractère volontaire de la démarche devrait primer sur une identité numérique imposée, dans laquelle le portefeuille ne serait qu'une extension volontaire de services pour des personnes auxquelles une identité numérique a été créée d'office. La numérotation choisie (18-1 et suivants), qui s'inscrit à la suite de l'article 18 sur les identifiants transmis par les fournisseurs d'identité, suggère cependant que le Gouvernement suive cette direction.

Cette solution conduirait à enrichir considérablement le Registre National Monégasque de l'Identité Numérique, conduisant à une gestion centralisée de l'identité numérique et donc à une concentration des risques. L'APDP s'inquiète ainsi, techniquement, de savoir s'il y aura une traçabilité centralisée de toutes les actions effectuées par les personnes utilisatrices, associée à des identifiants uniques et permanents. Cela induit pour l'APDP, d'une part un risque de suivi des comportements des utilisateurs, et, d'autre part, en cas de compromission d'un identifiant attribué à vie à la personne, une difficulté de réutilisation du système en cas de compromission.

b) Sur l'interopérabilité et la territorialité du dispositif

L'APDP s'interroge également sur la potentielle relation entre identité numérique monégasque et identité numérique européenne. Le portefeuille d'identité numérique européenne est, à des fins de sécurité dans les conditions d'enrôlement, réservé aux nationaux et résidents des pays membres. Le portefeuille d'identité numérique monégasque - s'il dépend de l'identité numérique monégasque - est ouvert quant à lui à des personnes figurant dans des traitements de l'Etat sélectionnés par Ordonnance Souveraine, tels que, par exemple, certaines personnes inscrites auprès de la Direction du Travail. Une reconnaissance mutuelle des portefeuilles est-elle envisageable eu égard à cette différence de personnes éligibles ?

A cet égard, l'APDP rappelle qu'en application de l'article 5 de la Loi n° 1.383, précitée, une identité numérique est automatiquement accordée à la personne figurant sur un registre éligible, sans qu'il soit précisé s'il sera vérifié en amont que les données qui y figurent sont exactes.

En outre, elle s'interroge sur de potentiels registres rendus éligibles mais ne contenant à l'origine que peu d'informations, qui nécessiteraient une collecte d'informations complémentaires pour octroyer l'identité numérique. Cette collecte, sans lien avec la finalité du registre, serait contraire aux dispositions de la Loi n° 1.565.

De plus, si les systèmes sont à terme interopérables, l'APDP constate qu'un travailleur frontalier aura une identité numérique monégasque obligatoire alors qu'il peut, dans son pays, en bénéficier d'une facultative présentant les mêmes avantages. Elle estime donc qu'il serait opportun que le législateur précise les scénarios qui sont envisagés, les calendriers prévisionnels, et les raisons pour lesquelles l'identité numérique serait rendue obligatoire pour toutes les personnes « *présentes dans un registre public* ».

En tout état de cause, l'APDP appelle l'attention sur l'application de l'article 35 de la Loi n° 1.565 relatif à l'analyse d'impact qui s'applique dès lors qu'un traitement permet l'utilisation à grande échelle d'un identifiant numérique.

Enfin, concernant la territorialité du dispositif, l'APDP constate que le portefeuille d'identité numérique permet de « *signaler une partie utilisatrice à la Commission de contrôle des Informations Nominatives lorsqu'une demande de données présumée illégale ou suspecte est reçue* », encrant territorialement le contrôle de la protection des données personnelles en Principauté. Toutefois, rien ne vient encadrer comment on demande à être une partie

utilisatrice, ni que la partie utilisatrice doit être établie en Principauté. Une société française limitrophe pourrait-elle demander à être une partie utilisatrice ?

Elle signale par ailleurs qu'il y a désormais lieu de mentionner « *l'Autorité de Protection des Données Personnelles* » en lieu et place de la référence à « *la Commission de Contrôle des Informations Nominatives* ».

c) Sur les autres remarques en lien avec le portefeuille d'identité numérique

La première remarque s'inscrit dans le prolongement de la distinction identité numérique et son support (comme par exemple la carte d'identité monégasque) par rapport au portefeuille d'identité numérique.

L'APDP relève que les téléservices qui ont été soumis à la CCIN utilisant l'identité numérique collectent nécessairement l'ensemble des informations de l'identité numérique : nom/nom d'usage, prénoms, nom de naissance, sexe, date et heure de naissance, lieu de naissance, Autorité d'enregistrement (Mairie ou DSP). En outre, comme l'avait indiqué la CCIN dans ses délibérations, l'utilisateur de l'identité numérique monégasque ne dispose pas d'un accès à une interface l'informant de la collecte et de la traçabilité des consultations de ses données en lien avec l'utilisation de ladite identité numérique.

Le portefeuille veille quant à lui, en application de l'article 18-2 projeté, à une divulgation sélective des données et l'utilisateur peut accéder à un journal de toutes les transactions effectuées par ce biais. L'article 18-7 indique quant à lui que « *les utilisateurs exercent un contrôle total sur l'utilisation de portefeuille d'identité numérique et des données qui y figurent* ».

Aussi, l'APDP appuie ses arguments développés au point II a) de la présente délibération et plaide pour une identité numérique de choix dans laquelle la personne maîtrise les flux de données personnelles. Le portefeuille d'identité numérique permet *in fine*, quand cela est possible, la preuve à divulgation nulle de connaissance.

Le choix des personnes devrait être également possible sur les modalités d'accès à un service, notamment préexistant. L'APDP relève que l'article 18-8 en projet dispose que « *L'utilisation de portefeuille d'identité numérique a lieu sur une base volontaire. Les personnes physiques ou morales qui n'utilisent pas le portefeuille d'identité numérique ne sont en aucune façon limitées ou désavantagées dans l'accès aux services publics et privés ou dans l'accès au marché du travail et la liberté d'entreprise. Il reste possible d'accéder aux services publics et privés par d'autres moyens d'identification et d'authentification existants* ».

L'APDP en prend acte et recommande en outre que le recours obligatoire à une identité numérique forte soit justifié et limité. En ce qui concerne la faculté de conserver un recours physique pour accéder aux services publics, l'APDP estime que l'article 43 de l'Ordonnance Souveraine n° 3.413 devrait être consacré par la Loi, en précisant qu'une alternative physique sera toujours possible dans un cadre non professionnel (à l'inverse de ce que la CCIN avait pu connaître concernant le traitement automatisé d'informations nominatives ayant pour finalité « *Bénéficiaire d'une aide auprès du Fonds Bleu par une démarche en ligne* » ouvert aux professionnels).

Il devrait être également possible aux personnes concernées de choisir de ne pas être soumises à un outil biométrique. Aussi, il devrait nécessairement exister une alternative d'enrôlement en présentiel à une analyse biométrique par le biais d'une application mobile lors de la création d'un portefeuille d'identité numérique/d'une identité numérique. Cela pourrait être inscrit au sein du dispositif.

Enfin, les personnes concernées ne devraient pas avoir à utiliser leur identité numérique personnelle dans le cadre de démarches professionnelles, afin de bénéficier d'une réelle dissociation entre sphère privée et professionnelle, et d'éviter les risques inhérents à une double utilisation.

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

Le Président

Robert CHANAS