REPUBLIQUE DU NIGER

Fraternité-Travail-Progrès

LOI N° 2022-59

du 16 décembre 2022

relative à la protection des données à caractère personnel.

Vu la Constitution du 25 novembre 2010 ;

Vu la Convention de l'Union Africaine sur la cyber sécurité et la protection des données à caractère personnel ;

Vu l'Acte Additionnel A/SA.1/01/10 sur la protection des données à caractère personnel dans l'espace de la CEDEAO ;

LE CONSEIL DES MINISTRES ENTENDU ;

L'ASSEMBLEE NATIONALE A DÉLIBÉRÉ ET ADOPTÉ ;

LE PRESIDENT DE LA REPUBLIQUE PROMULGUE LA LOI DONT LA TENEUR SUIT :

CHAPITRE PREMIER : DEFINITIONS

Article premier : Au sens de la présente loi, on entend par :

- **Anonymisation :** tout procédé appliqué aux données à caractère personnel pour que les personnes concernées ne puissent plus être identifiées ni directement, ni indirectement de manière irréversible et par quelque moyen que ce soit ;
- **Activité de cryptologie** : toute activité ayant pour but la production, l'utilisation, l'importation, l'exportation ou la commercialisation des moyens de cryptologie ;
- **Agrément :** la reconnaissance formelle par un organisme agréé, que le produit ou le système évalué peut protéger jusqu'à un niveau spécifié ;
- **Archivage électronique sécurisé** : l'ensemble des modalités de conservation et de gestion des archives électroniques destinées à garantir leur valeur juridique pendant toute la durée nécessaire ;
- **Autorité de protection** : autorité administrative indépendante chargée de veiller à ce que les traitements des données à caractère personnel soient mis en œuvre conformément aux dispositions légales et règlementaires en la matière ;
- **Chiffrement** : toute technique qui consiste à transformer des données numériques en un format inintelligible en employant des moyens de cryptologie ;

- **Code de conduite** : tout document élaboré par le Responsable du Traitement et homologué par l'Autorité de protection, en conformité avec la présente loi, afin d'instaurer un usage correct des ressources informatiques, de l'Internet et des communications électroniques de la structure concernée ;

- **Communication électronique** : toute émission, transmission ou réception de signes, de signaux, d'écrits, d'images, de sons ou de vidéos par voie électromagnétique, optique ou par tout autre moyen ;

- **Consentement de la personne concernée** : toute manifestation de volonté expresse, libre, spécifique, éclairée et non équivoque par laquelle la personne concernée ou son représentant légal, judiciaire ou conventionnel accepte, par une déclaration ou par un acte positif clair, oralement ou par écrit, que des données la concernant fassent l'objet d'un traitement manuel ou électronique ;

- **Conventions secrètes** : toutes clés non publiées, nécessaires à la mise en œuvre d'un moyen ou d'une prestation de cryptologie pour les opérations de chiffrement ou de déchiffrement ;

- **Correspondant :** la personne désignée par la structure procédant à un traitement des données à caractère personnel et à laquelle peut s'adresser toute personne concernée par une question y relative et qui joue le rôle d'interface entre le responsable de traitement et l'autorité de protection ;

- **Cryptologie** : la science relative à la protection et à la sécurité des informations notamment pour la confidentialité, l'authentification, l'intégrité et la non répudiation ;

- **Destinataire d'un traitement de données à caractère personnel** : toute personne physique ou morale publique ou privée, habilitée à recevoir une communication de ces données, autre que la personne concernée, le Responsable du Traitement, le sous-traitant et les personnes qui, en raison de leurs fonctions, sont chargés de traiter des données ;

- **Disparition forcée :** l'arrestation, la détention, l'enlèvement ou toute autre forme de privation de liberté par des agents de l'État ou par des personnes ou des groupes de personnes qui agissent avec l'autorisation, l'appui ou l'acquiescement de l'État, suivi du déni de la reconnaissance de la privation de liberté ou de la dissimulation du sort réservé à la personne disparue ou du lieu où elle se trouve, la soustrayant à la protection de la loi ;

- **Document :** le résultat d'une série de lettres, de caractères, de chiffres, de figures ou de tous autres signes ou symboles qui a une signification intelligible, quelles que soient leurs modalités de transmission ;

- **Données à caractère personnel** : toute information de quelque nature qu'elle soit et indépendamment de son support, y compris le son et l'image, relative à une personne physique identifiée ou identifiable directement ou indirectement, par référence à un numéro d'identification ou à plusieurs éléments spécifiques, propres à son identité physique, physiologique, génétique, psychique, culturelle, sociale ou économique ;

- **Données informatisées** : toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire exécuter une fonction par un système d'information ;

- **Données de localisation ou informations de localisation** : toutes les données traitées dans un réseau de communications électroniques indiquant la position géographique de l'équipement terminal d'un utilisateur final d'un service de communications électroniques accessible au public. Dans le cas d'un réseau fixe public, les données sont celles relatives à l'adresse physique du point de terminaison du réseau ;

- **Données relatives au trafic** : toutes données ayant trait à une communication passant par un système d'information, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type de service sous-jacent ;

- **Données sensibles** : toutes données à caractère personnel relatives aux opinions ou activités religieuses, philosophiques, politiques, syndicales, à la vie sexuelle ou raciale, à la santé, aux mesures d'ordre social, aux poursuites, aux sanctions pénales ou administratives ;

- **Données de santé :** toutes données à caractère personnel relatives à la santé physique ou mentale d'une personne, y compris la prestation de services de soins de santé qui révèle des informations sur l'état de santé passé, actuel et futur de cette personne ;

- **Données de transit** : toutes données utilisées temporairement dans le cadre des activités techniques, notamment de stockage, de transmission, de fourniture, d'accès à un réseau numérique, aux fins de permettre à d'autres destinataires du service la meilleure utilisation ;

- **Données biométriques :** toutes 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 ;

- **Données génétiques :** toutes données concernant les caractères héréditaires d'un individu ou d'un groupe d'individus apparentés ;

- **Echange de données informatisées (EDI)** : tout transfert électronique d'une information d'un système électronique à un autre mettant en œuvre une norme convenue pour structurer l'information ;

- **Ecrit** : toute suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles qui a une signification intelligible, quels que soient leurs supports et leurs modalités de transmission ;

- **Fichier de données à caractère personnel** : tout ensemble structuré de données accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou reparti de manière fonctionnelle ou géographique, permettant d'identifier une personne déterminée ;

- **Garanties appropriées** : toutes mesures techniques ou organisationnelles, volontaires ou imposées par la présente loi, destinées à assurer la sécurité des données et le respect des principes de traitement des données à caractère personnel ;

- **Identité :** l'adresse postale ou géographique, le numéro de téléphone et tout autre numéro d'accès, les informations relatives à la localisation, à la facturation et à l'endroit où se trouvent les équipements de communication ;

- **Identité numérique** : ensemble de traces numériques qu'une personne ou une entité laisse sur internet. Toutes ces informations laissées au fil des navigations sont collectées par les moteurs de recherche et sont rendues publiques (pseudo, noms, images, vidéos, adresses IP, favoris, etc.) ;

- **Information** : tout élément de connaissance susceptible d'être représenté à l'aide de conventions, pour être utilisé, conservé, traité ou communiqué. L'information peut être exprimée sous forme écrite, visuelle, sonore, numérique, etc. ;

- **Intelligence artificielle** : ensemble de sciences, théories et techniques dont le but est de reproduire, par une machine, des capacités cognitives d'un être humain ;

- **Interconnexion de fichiers ou de bases de données** : tout mécanisme de connexion consistant en la mise en relation de données traitées pour une finalité déterminée avec d'autres données traitées pour des finalités identiques ou non, ou liées par un ou plusieurs responsable(s) de traitements ;

- **Internet des objets** : désigne l'évolution technologique, où les objets traditionnellement non connectés, qu'ils soient physiques ou virtuels, auront désormais la capacité de communiquer entre eux en temps réel ;

- **Méga-données** : ensemble des données à caractère personnel ou non, générées par les nouvelles technologies de l'information et de la communication, caractérisées par leur volume colossal ;

- **Message électronique :** toute information créée, envoyée, reçue ou conservée par des moyens électroniques ou optiques ou des moyens analogues, notamment, mais non exclusivement, l'échange de données informatisées (EDI), la messagerie électronique, le télégraphe, le télex et la télécopie ;

- **Migrants** : ce terme désigne aussi bien les émigrants nigériens, que les immigrés vivant ou en transit au Niger. Ce terme inclut également les réfugiés, les demandeurs d'asile et les travailleurs internationaux ;

- **Mineur ou Enfant** : toute personne âgée de moins de dix-huit (18) ans conformément aux dispositions légales en vigueur ;

- **Moyens de cryptologie** : l'ensemble des outils scientifiques et techniques (matériel ou logiciel) qui permettent de chiffrer et/ou de déchiffrer. On entend également par moyen de cryptologie tout matériel ou logiciel conçu ou modifié pour transformer des données, qu'il s'agisse d'écrits ou de signaux, à l'aide de conventions secrètes ou non ;

- **Non répudiation** : faculté de ne pas contester l'authenticité de l'information sécurisée ou cryptée ;

- **Oubli numérique** : fait allusion au devoir de prendre les dispositions qui s'imposent pour effacer ou rendre les données à caractère personnel indisponibles lorsqu'il n'est plus nécessaire de les garder ou lorsqu'aucune finalité légitime ne justifie leur conservation ;

- **Outil de conformité** : ensemble d'instruments prévus par les textes permettant aux responsables de traitement de gérer leur conformité d'une façon dynamique et de démontrer qu'ils respectent la règlementation : registre des traitements, analyse d'impact sur la protection des données personnelles, référentiels, certifications, etc.

- **Pays tiers** : tout Etat non membre de la CEDEAO ;

- **Personne concernée** : toute personne physique dont les données font l'objet d'un traitement des données à caractère personnel ;

- **Prestation de cryptologie** : toute opération visant à la mise en œuvre, pour le compte de soi ou d'autrui, des moyens de cryptologie ;

- **Prestataire de service de cryptologie :** toute personne, physique ou morale, qui fournit une prestation de cryptologie ;

- **Profilage** : tout traitement automatisé de données à caractère personnel en vue d'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 ;

- **Prospection directe** : toute sollicitation effectuée au moyen de l'envoi de message, quel qu'en soit le support ou la nature notamment commerciale, politique ou caritative, destinée à promouvoir, directement ou indirectement, des biens, des services ou l'image d'une personne ou d'une organisation ;

- **Pseudonymisation** : traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne sans avoir recours à des informations supplémentaires ;

- **Règles contraignantes d'entreprise** : un code de conduite homologué par l'Autorité de protection, par lequel un groupe de sociétés définit sa politique interne en matière de transferts de données à caractère personnel ;

- **Représentant** : toute personne physique ou morale établie au Niger, désignée, par le responsable du traitement ou le sous-traitant, en vertu d'une convention, pour le représenter ;

- **Responsable du Traitement** : la personne physique ou morale, publique ou privée, tout autre organisme ou association qui, seul ou conjointement avec d'autres, prend la décision de collecter et de traiter des données à caractère personnel et en détermine les finalités ;

- **Système de vidéosurveillance** : dispositif de captation d'image statique et/ou animée placé dans un lieu public ou privé pour visualiser en un endroit centralisé ou non tous les flux de personnes et autres objets mobiles afin de prévenir les vols, agressions et mouvements de foule ou tout autre source potentielle d'insécurité ;

- **Système d'information** : tout dispositif humain et/ou électronique, isolé ou interconnecté, assurant en tout ou partie, un traitement manuel et/ou automatisé d'informations ;

- **Sous-traitant** : toute personne physique ou morale, publique ou privée, tout autre organisme ou association qui traite des données à caractère personnel pour le compte du Responsable du Traitement ;

- **Technologies de l'Information et de la Communications (TIC) :** technologies employées pour recueillir, stocker, utiliser et envoyer des informations et incluant celles qui impliquent l'utilisation des ordinateurs ou de tout système de communications y compris les télécommunications ;

- **Télésurveillance :** tout procédé de surveillance à distance faisant recours à l'utilisation des technologies de l'information et de la communication. Il inclut la vidéosurveillance ;

- **Tiers** : toute personne physique ou morale, publique ou privée, tout autre organisme ou association autre que la personne concernée, le Responsable du Traitement, le sous-traitant et les personnes qui, placés sous l'autorité directe du Responsable du Traitement ou du sous-traitant, sont habilités à intervenir et à traiter les données ;

- **Traitement de données à caractère personnel** : toute opération ou ensemble d'opérations, effectuées à l'aide de procédés automatisés ou non et appliqués à des données, telles que la collecte, l'exploitation, l'enregistrement, l'organisation, la conservation, l'adaptation, la modification, l'extraction, la sauvegarde, la copie, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, le cryptage, l'effacement ou la destruction des données à caractère personnel ;

- **Violation de données à caractère personnel** : toute 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.

Les définitions des instruments juridiques de la CEDEAO, de l'Union Africaine ou de l'Union Internationale des Télécommunications prévalent pour les termes non définis par la présente loi.

CHAPITRE II : DE L'OBJET ET DU CHAMP D'APPLICATION

Article 2 : Objet

La présente loi fixe les principes et les règles régissant la protection des personnes physiques en ce qui concerne le traitement de leurs données à caractère personnel.

Elle garantit que tout traitement, sous quelque forme que ce soit et le mode d'exécution utilisé respecte les libertés et droits fondamentaux des personnes physiques, notamment le droit à la vie privée.

Elle crée une autorité nationale chargée de la protection des données à caractère personnel.

Article 3 : Champ d'application matériel

Sont soumis à la présente loi :

1. toute collecte, tout traitement, toute transmission, tout stockage et toute utilisation des données à caractère personnel par des personnes morales de droit public ou de droit privé ainsi que par des personnes physiques ;

2. tout traitement automatisé ou non de données à caractère personnel contenues ou appelées à figurer dans un fichier, mis en œuvre par des personnes morales de droit public ou de droit privé ainsi que par des personnes physiques ;

3. tout traitement de données concernant la sécurité publique, la défense, la recherche et la poursuite d'infractions pénales ou la sûreté de l'État, sous réserve des dérogations définies par la présente loi ou d'autres lois en vigueur.

Article 4 : Champ d'application territorial

La présente loi s'applique aux traitements de données à caractère personnel mis en œuvre par :

- un responsable du traitement ou un sous-traitant établi sur le territoire national et en tout lieu où la présente loi s'applique ;

- un responsable du traitement ou un sous-traitant non établi au Niger, qui recourt à des moyens de traitement situés sur le territoire national, à l'exclusion des moyens qui ne sont utilisés qu'à des fins de transit sur le territoire. Lorsqu'il n'est pas établi au Niger, le responsable du traitement doit désigner un représentant établi sur le territoire national, nonobstant les recours qui peuvent être introduits directement à son encontre ;

- un responsable du traitement ou un sous-traitant non établi au Niger, lorsque l'activité de traitement vise des citoyens nigériens ou l'offre de biens et services à des personnes établies au Niger.

Article 5 : Exclusions du champ d'application

La présente loi ne s'applique pas :

- aux traitements de données mis en œuvre par une personne physique dans le cadre exclusif de ses activités personnelles ou domestiques, à condition toutefois que les données collectées ne soient pas destinées à une communication systématique à des tiers ou à la diffusion ;

- aux copies temporaires 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 et à seule fin de permettre à d'autres destinataires du service le meilleur accès possible aux informations transmises ;

- aux traitements de données à caractère personnel effectués à des fins littéraires et artistiques ou à des fins de journalisme, quel que soit le média utilisé, dans le respect des règles déontologiques et éthiques de ces professions et des règles de modération obligatoires applicables aux forums de discussion ou autres supports de diffusion.

CHAPITRE III : DE L'AUTORITE DE PROTECTION DES DONNEES A CARACTERE PERSONNEL

Article 6 : Création et Statut

Il est créé auprès du Premier Ministre une Haute Autorité de Protection des Données à caractère Personnel en abrégé « HAPDP ».

La HAPDP est une autorité administrative indépendante chargée de veiller à la conformité des traitements des données à caractère personnel aux dispositions des textes en vigueur et des conventions internationales auxquelles le Niger est partie.

Elle est dotée de la personnalité morale et de l'autonomie financière.

Le siège de la HAPDP est fixé à Niamey.

La HAPDP peut créer en cas de besoin des démembrements à l'intérieur du pays.

Article 7 : Composition

La HAPDP est composée de **neuf (09)** membres, choisis, en raison de leur compétence juridique et/ou technique, ainsi qu'il suit :

- deux (2) personnalités désignées par le Premier ministre ;
- un (1) magistrat membre de la Cour de Cassation désigné par le Premier Président de la Cour de Cassation ;
- un (1) magistrat membre du Conseil d'Etat désigné par le Premier Président du Conseil d'Etat ;
- un (1) avocat désigné par l'Ordre des avocats ;
- un (1) médecin désigné par l'ordre des Médecins ;
- un (1) représentant élu par le collectif des organisations de défense des droits de l'homme ;
- deux (2) experts en TIC dont un (1) désigné par le Ministre chargé des Technologies de l'Information et de la Communication et un (1) désigné par l'Agence Nationale pour la Société de l'Information (ANSI).

Article 8 : Mandat, nomination et rémunération

Les membres de la HAPDP sont nommés par décret pris en Conseil des Ministres pour un mandat de cinq (5) ans renouvelables une fois. Il est pourvu au remplacement des membres soixante (60) jours au moins avant l'expiration de leur mandat.

En cas de décès ou de démission volontaire ou d'office d'un membre, il est pourvu à son remplacement dans les soixante (60) jours, dans les conditions prévues à l'article 7 ci-dessus. Le mandat du remplaçant est limité au temps restant à courir.

La HAPDP est dirigée par un Président nommé parmi ses membres par décret pris en Conseil des Ministres.

Le Président de la HAPDP est secondé par un vice-président élu par ses pairs.

A l'exception du Président, les membres de la HAPDP n'exercent pas leur fonction à titre permanent.

En cas de vacance dûment constatée du Président, le vice-Président assume provisoirement les fonctions de Président.

Avant d'entrer en fonction les membres de la HAPDP prêtent devant la Cour de Cassation le serment dont la teneur suit : « ***Je jure solennellement de bien et fidèlement remplir ma fonction de membre de la Haute Autorité de Protection des Données à caractère Personnel, en toute indépendance et impartialité de façon digne et loyale et de garder le secret des délibérations***».

La durée du mandat des membres de la HAPDP court à partir de la date de prestation du serment.

Le Président de la HAPDP perçoit une rémunération dont le montant est fixé par décret pris en Conseil des Ministres.

Les membres de la HAPDP reçoivent des indemnités dont le montant est fixé par décret pris en Conseil des Ministres.

Article 9 : Irrévocabilité du mandat de membre de la HAPDP

Le mandat des membres de la HAPDP est irrévocable.

Toutefois, Il peut être mis fin à la fonction de membre de la HAPDP en cas de décès, de démission, de manquement grave à une obligation légale ou à une incapacité définitive empêchant la poursuite de son mandat constatés par la HAPDP dans les conditions définies par son règlement intérieur.

Article 10 : Immunité et indépendance des membres de la HAPDP

Les membres de la HAPDP jouissent d'une immunité totale pour les opinions émises dans l'exercice ou à l'occasion de l'exercice de leurs fonctions.

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

Article 11 : Incompatibilités

La qualité de membre de la HAPDP est incompatible avec la qualité de membre du Gouvernement, l'exercice de fonctions de dirigeants d'entreprise du secteur des technologies de l'information et de la communication ainsi que la détention de participation dans lesdites entreprises.

Tout membre de la HAPDP doit informer celle-ci de tous autres intérêts directs ou indirects qu'il détient ou vient à détenir, de toutes autres fonctions qu'il exerce ou vient à exercer et de tout mandat qu'il détient ou vient à détenir au sein des entreprises du secteur des technologies de l'information et de la communication. En cas de besoin, la HAPDP prend

toutes les dispositions utiles pour assurer l'indépendance et l'impartialité de ses membres. Un code de conduite est élaboré par la HAPDP à cet effet.

Après la cessation de leurs fonctions, les membres de la HAPDP sont tenus de respecter les devoirs d'honnêteté et de délicatesse quant à l'acceptation de fonctions ou d'avantages incompatibles avec la qualité d'anciens membres de cette institution.

Article 12 : Secret professionnel

Les membres de la HAPDP sont tenus au secret professionnel pour les informations confidentielles dont ils ont eu connaissance dans le cadre ou à l'occasion de l'exercice de leurs fonctions, y compris après la cessation de leurs fonctions.

Les agents et les experts commis par la HAPDP sont également soumis, y compris après cessation de leurs activités, à l'obligation de secret professionnel pour toute information confidentielle, fait et acte dont ils ont eu connaissance dans l'exercice de leurs missions.

Les responsables du traitement des données à caractère personnel et les prestataires de service de cryptologie agissant dans le cadre de l'accomplissement de leurs activités ne peuvent opposer à la HAPDP le secret professionnel auquel ils sont assujettis.

Article 13 : Exception au secret professionnel

Les informaticiens ou tout autre agent d'une entreprise, appelés à donner les renseignements à la HAPDP ou à témoigner devant elle, sont déliés de leur obligation de respect du secret professionnel.

Ils ne peuvent subir ni intimidation, ni menace, ni être poursuivis ou sanctionnés.

Article 14 : Commissaire du gouvernement :

Un Commissaire du gouvernement siège auprès de la HAPDP.

Le Commissaire du gouvernement est choisi parmi les personnalités reconnues pour leur compétence en matière juridique ou administrative relevant de la catégorie A1 du statut général de la fonction publique de l'Etat et ayant au moins dix (10) ans d'ancienneté.

Il est nommé par décret pris en Conseil des ministres, sur proposition du Premier Ministre.

Il est mis fin à ses fonctions dans les mêmes conditions.

Le Commissaire du gouvernement informe la HAPDP sur les orientations du Gouvernement et sur les attentes de l'administration concernant la mise en œuvre des traitements des données à caractère personnel.

Les missions du Commissaire du Gouvernement sont précisées par décret pris en Conseil des Ministres.

Le Commissaire du gouvernement est convoqué à toutes les sessions de la HAPDP dans les mêmes conditions que les membres de celle-ci. Il ne prend pas part au vote.

En cas d'empêchement, le Commissaire du gouvernement peut adresser des observations écrites au Président de la HAPDP, avant la session, sur les sujets et les projets de délibérations inscrits à l'ordre du jour.

Le Commissaire du gouvernement bénéficie des avantages prévus par décret pris en Conseil des Ministres.

Avant d'entrer en fonction le Commissaire du gouvernement, prête serment devant la Cour de Cassation en ces termes : ***« Je jure solennellement de bien et fidèlement remplir ma fonction de Commissaire du gouvernement. Je ne révélerai et ne ferai connaître, sans y être autorisé par la loi, aucun renseignement confidentiel dont j'aurai eu connaissance dans l'exercice de mes fonctions*** ».

<u>Article 15 :</u> Missions de la HAPDP

La HAPDP est chargée de veiller à ce que les traitements des données à caractère personnel soient mis en œuvre conformément aux dispositions de la présente loi et des autres textes législatifs et réglementaires contenant des dispositions relatives à la protection des données à caractère personnel.

Elle veille à ce que le traitement et l'usage des données à caractère personnel ne porte pas atteinte aux libertés publiques ou ne comporte pas de menace à la vie privée des citoyens, en particulier dans l'utilisation des technologies de l'information et de la communication.

A ce titre, elle est chargée notamment :

- de prendre, sous forme de délibération, des décisions individuelles ou réglementaires dans les cas prévus par la présente loi ;
- d'édicter, le cas échéant, des recommandations en vue de faciliter l'application de la présente loi ;
- d'informer les personnes concernées et les responsables de traitement de leurs droits et obligations ;
- de recevoir les déclarations, les demandes d'avis et les demandes d'autorisation pour la mise en œuvre de traitement de données à caractère personnel, ou de les retirer dans les cas prévus par la présente loi ;
- de recevoir les réclamations, les dénonciations, les pétitions et les plaintes relatives à la mise en œuvre des traitements de données à caractère personnel et d'informer les auteurs de la suite donnée à celles-ci ;

- de conseiller les personnes physiques ou morales qui procèdent à des traitements des données à caractère personnel ou à des essais ou expériences de nature à aboutir à de tels traitements ;
- d'informer sans délai, l'autorité judiciaire compétente des infractions dont elle a connaissance dans le cadre de ses missions ;
- de déterminer, en cas de besoin, les garanties nécessaires et prendre les mesures appropriées pour la protection des données à caractère personnel ;
- d'autoriser, dans les conditions fixées par décret pris en Conseil des Ministres, le transfert transfrontalier des données à caractère personnel ;
- de procéder par l'intermédiaire des agents assermentés, à des opérations de contrôle portant sur tout traitement et, le cas échéant, d'obtenir des copies de tout document ou support d'information utile à sa mission ;
- d'assurer en permanence l'information, la sensibilisation et la formation du public afin de promouvoir le droit à la protection des données à caractère personnel ;
- de valider et d'homologuer les chartes d'utilisation qui lui sont présentées ;
- de mettre à jour et de tenir à la disposition du public, pour consultation, un répertoire de traitement de données à caractère personnel ;
- de répondre à toute demande d'avis portant sur le traitement de données à caractère personnel ;
- de donner un avis motivé sur tout projet ou proposition de loi ou projet de textes règlementaires relatifs au traitement de données à caractère personnel ;
- de présenter au Gouvernement toute suggestion susceptible de simplifier et d'améliorer le cadre législatif et réglementaire relatif au traitement des données à caractère personnel ;
- de répondre aux demandes d'avis des organismes privés et des personnes concernées sur toute question en relation avec les dispositions de la présente loi et ses textes d'application ;
- de répondre aux demandes d'avis des autorités judiciaires sur les éléments soumis à leur appréciation lors des contentieux relatifs à la protection de données à caractère personnel ;
- d'élaborer les règles de conduite relative au traitement et à la protection des données à caractère personnel ;
- d'établir et de publier les lignes directrices, les recommandations ou les référentiels destinés à faciliter la mise en conformité des traitements de données à caractère personnel avec la présente loi ;
- de participer aux activités de recherche scientifique, de formation et d'étude en rapport avec la protection des données à caractère personnel, et d'une manière générale avec les libertés et la vie privée ;
- d'ordonner la rectification, l'effacement ou la destruction de toutes les données lorsqu'elles ont été traitées en violation des dispositions de la présente loi ainsi que la notification de ces mesures aux tiers auxquels les données ont été divulguées ;

- de prononcer les sanctions administratives et pécuniaires à l'encontre des responsables de traitement en cas de manquements aux dispositions de la présente loi ;
- de mettre en place les mécanismes de coopération avec les autorités de protection des données à caractère personnel des autres pays ;
- de participer aux négociations internationales en matière de protection des données à caractère personnel.

La HAPDP établit son règlement intérieur qui précise, notamment, les règles relatives aux délibérations, à l'instruction, et à la présentation des dossiers.

La HAPDP présente chaque année au Président de la République, au Président de l'Assemblée Nationale et au Premier ministre un rapport public rendant compte de l'exécution de sa mission.

Article 16 : Pouvoir réglementaire

En vertu du pouvoir règlementaire dont elle dispose, la HAPDP peut, notamment édicter et publier des lignes directrices, des référentiels, ou prendre des délibérations de portée générale pour préciser les modalités pratiques de la mise en œuvre de certaines dispositions de la présente loi.

Article 17 : Obligation de collaboration

Les autorités publiques, les dirigeants des entreprises publiques ou privées, les responsables de structures diverses concernées par le traitement des données à caractère personnel, les détenteurs et les utilisateurs de fichiers de données à caractère personnel ne peuvent entraver l'action de la HAPDP. Ils doivent prendre toutes mesures utiles afin de lui faciliter l'accomplissement de sa mission.

Article 18 : Organes de la HAPDP

Les organes de la HAPDP sont :

- la Plénière composée des membres de la HAPDP cités à l'article 7 ci-dessus qui en est l'organe délibérant ;
- l'administration, comprenant le président de la HAPDP et le secrétariat général, qui en est l'organe exécutif.

Article 19 : Plénière de la HAPDP

La Plénière est l'instance d'orientation, de décision et de délibération de la HAPDP.

La Plénière de la HAPDP se réunit tous les deux (2) mois en session ordinaire.

Elle peut se réunir en session extraordinaire chaque fois que de besoin.

Les sessions ordinaires et extraordinaires de la plénière sont convoquées et présidées par le Président de la HAPDP.

La plénière de la HAPDP délibère et approuve :

- le règlement intérieur de la HAPDP ;
- les dossiers de demandes d'avis, de demandes d'autorisation de traitement et de demandes d'autorisation de transfert de données vers un pays tiers ;
- les rapports des missions de contrôle du respect de la réglementation sur la protection des données à caractère personnel ;
- les projets de sanctions pour non-respect de la réglementation sur la protection des données à caractère personnel ;
- les programmes d'activités annuels et pluriannuels de la HAPDP ;
- les budgets annuels des programmes d'investissements pluriannuels de la HAPDP ;
- les états financiers de fin d'exercice de la HAPDP ;
- le rapport annuel d'activités de la HAPDP ;
- le manuel de procédures administratives, comptables, financières et techniques de la HAPDP ;
- l'organisation des services de la HAPDP ;
- le projet de statut du personnel de la HAPDP.

La plénière de la HAPDP délibère également sur toute autre question relevant de la protection des données à caractère personnel.

La plénière de la HAPDP exerce collégialement ses attributions et ne délibère valablement qu'en présence de deux tiers (2/3) de ses membres.

La plénière prend ses décisions à la majorité simple des membres présents. En cas d'égalité de voix, celle du Président est prépondérante.

Le secrétariat des sessions de la HAPDP est assuré par le Secrétaire Général ou par tout autre agent désigné par le Président en cas d'empêchement.

Article 20 : Président de la HAPDP

Le Président de la HAPDP dispose des pouvoirs nécessaires à la bonne marche de la HAPDP et veille à l'exécution des décisions prises par la Plénière.

A ce titre, il est notamment chargé de :

- convoquer et présider les sessions de la plénière ;
- préparer et soumettre pour adoption à la plénière, le budget et les programmes d'activités ;
- exécuter les programmes d'activités et le budget en qualité d'ordonnateur ;
- soumettre à la plénière, au plus tard le 31 mars de l'année suivante, l'état d'exécution du budget précédent ;
- soumettre à la plénière pour examen et adoption dans les cinq (5) mois suivant la fin de la gestion, les états financiers arrêtés ;

- préparer et soumettre pour adoption à la plénière l'organigramme de la HAPDP, le projet de statut du Personnel, le manuel des procédures et le règlement intérieur de la HAPDP ;
- recruter et nommer le personnel de la HAPDP ;
- représenter la HAPDP en justice et dans tous les actes de la vie civile ;

En outre, la plénière peut, en cas de nécessité lui déléguer certaines de ses attributions.

Article 21 : Administration de la HAPDP

Le Président est le chef de l'administration de la HAPDP.

A ce titre, il dispose d'un cabinet composé de :

- un chef de cabinet ;
- un secrétaire particulier ;
- un chargé de communication ;
- un agent de protocole ;
- trois conseillers techniques choisis en raison de leurs compétences en matière juridique, administrative ou des TIC.

La HAPDP dispose d'un secrétariat général, des directions et des services dont l'organisation et les attributions sont approuvées par délibération de la Plénière.

Le Secrétariat général est dirigé par un secrétaire général placé sous l'autorité du Président.

Le Secrétaire général est choisi parmi les personnalités reconnues pour leur compétence en matière juridique, administrative ou des TIC relevant de la catégorie A1 du statut général de la fonction publique de l'Etat et ayant au moins dix (10) ans d'ancienneté.

II est nommé par décret pris en Conseil des Ministres, sur proposition du président de la HAPDP.

Les traitements de base, les indemnités et les autres avantages alloués au Secrétaire général de la HAPDP ainsi qu'aux responsables des directions et services placés sous son autorité sont fixés par décret pris en Conseil des Ministres.

Le Secrétaire général de la HAPDP prête serment devant la Cour d'Appel de Niamey en ces termes : « *Je jure solennellement de bien et fidèlement remplir ma fonction de Secrétaire général de la Haute Autorité de Protection des Données à Caractère Personnel. Je ne révélerai et ne ferai connaître, sans y être autorisé par la loi, aucun renseignement confidentiel dont j'aurai eu connaissance dans l'exercice de mes fonctions* ».

Article 22 : Personnel de la HAPDP

La HAPDP recrute son personnel de direction, d'encadrement et de contrôle par appel à candidatures sur la base des compétences et des qualifications techniques.

Il peut être mis à sa disposition et à sa demande des fonctionnaires de l'Etat par voie de détachement ou de mise à disposition.

Le statut du personnel, la grille de traitement de base, les primes, les indemnités et les autres avantages accordés au personnel administratif et technique sont fixés par décret pris en Conseil des Ministres.

Le personnel de la HAPDP est soumis à un règlement intérieur adopté par la Plénière des membres.

CHAPITRE IV : DES DISPOSITIONS FINANCIERES ET COMPTABLES

Article 23 : Ressources de la HAPDP

La HAPDP dispose de ressources ordinaires et de ressources exceptionnelles.

Constituent les ressources ordinaires de la HAPDP :

- la subvention de l'Etat ;
- 5% du fonds d'investissement pour le développement recouvré par l'ARCEP ;
- 5% du fonds d'accès universel aux services de communication électronique ;
- les frais de délivrance des autorisations et des récépissés aux responsables de traitement ;
- les subventions et concours des organismes publics autres que l'Etat ;
- les appuis des partenaires au développement ;
- les produits des travaux et des prestations qu'elle exécute.

Constituent les ressources exceptionnelles de la HAPDP :

- les produits des amendes et condamnations pécuniaires ;
- les produits des emprunts autorisés par l'Etat ;
- les produits financiers et les subventions des organismes publics ou privés nationaux ou internationaux ;
- les dons et legs régulièrement autorisés ;
- toute autre ressource autorisée par les lois et règlements.

Les ressources ordinaires sont mises en recouvrement et recouvrées par la HAPDP. Les paiements correspondants sont versés sur des comptes courants ouverts au nom de la HAPDP.

Les modalités de recouvrement et d'affectation des amendes et condamnations pécuniaires sont fixées par décret pris en Conseil des Ministres.

Elle est soumise au Code des marchés publics et des délégations de service public en ce qui concerne les règles de passation, d'exécution et de contrôle des marchés.

Les fonds de la HAPDP, provenant des conventions et des accords internationaux sont gérés suivant les modalités prévues par ces conventions et ces accords.

La HAPDP élabore un manuel de procédures administratives, financières, techniques et comptables.

Article 24 : Budget de la HAPDP

La HAPDP élabore et adopte son budget. L'exercice budgétaire court du 1er janvier au 31 décembre.

Le budget de la HAPDP prévoit et autorise les recettes et les dépenses dont il détermine la nature et le montant. Le Président de la HAPDP en est l'ordonnateur.

La HAPDP applique les règles de la comptabilité publique.

Le budget de la HAPDP adopté par la Plénière des membres est transmis au Premier Ministre pour approbation.

Article 25 : Frais de délivrance des autorisations et récépissés

La délivrance des autorisations et des récépissés pour la mise en œuvre des traitements des données à caractère personnel donne lieu à la perception des frais annuels au profit de la HAPDP dont les montants sont fixés par décret pris en Conseil des Ministres.

Article 26 : Affectation des ressources

Les ressources perçues par la HAPDP ou mises à sa disposition sont utilisées pour financer les activités concourant à la réalisation de sa mission.

Article 27 : Etats financiers

Les états financiers annuels sont transmis à la Cour des Comptes six (6) mois après la fin de l'exercice.

Article 28 : Contrôle des comptes

Les comptes de la HAPDP sont soumis au contrôle de la Cour des Comptes, de l'Inspection Générale des Finances et ainsi qu'à celui de l'Inspection Générale d'Etat.

CHAPITRE V : DES FORMALITES NECESSAIRES AU TRAITEMENT DES DONNEES A CARACTERE PERSONNEL

Article 29 : Formalités préalables

Sauf dispositions législatives contraires, le traitement des données à caractère personnel est soumis à une formalité préalable auprès de la HAPDP.

La formalité comporte l'engagement que le traitement satisfait aux exigences de la loi.

La HAPDP délivre un récépissé en réponse à la déclaration, le cas échéant, par voie électronique. Le demandeur peut mettre en œuvre le traitement dès réception de son récépissé. Il n'est exonéré d'aucune de ses responsabilités.

Les traitements relevant d'un même organisme et ayant des finalités identiques ou liées entre elles peuvent faire l'objet d'une déclaration unique. Les informations requises au titre de la déclaration ne sont fournies pour chacun des traitements que dans la mesure où elles lui sont propres.

L'accomplissement de cette formalité obligatoire se traduit par le dépôt d'un dossier de déclaration, de demande d'autorisation ou d'avis.

Les modalités de dépôt de demande d'avis, de déclarations ou d'octroi des autorisations pour le traitement des données à caractère personnel conformément aux dispositions de la présente loi sont fixées par décret pris en Conseil des Ministres.

Article 30 : Règles communes aux formalités

La demande d'avis, la déclaration et la demande d'autorisation sont adressées à la HAPDP et contiennent obligatoirement les mentions suivantes :

- l'identité, le domicile, l'adresse postale ou géographique du responsable du traitement ou si celui-ci n'est pas établi sur le territoire national, celles de son représentant dûment mandaté, et s'il s'agit d'une personne morale, sa dénomination sociale, son siège social, l'identité de son représentant légal, son numéro d'immatriculation au registre du commerce et du crédit mobilier, son numéro de déclaration fiscale ;
- la ou les finalités du traitement ainsi que la description générale des fonctions du requérant ;
- les interconnexions envisagées ou toutes autres formes de mise en relation avec d'autres traitements ;
- la catégorie des données à caractère personnel traitées, leur origine et les catégories de personnes concernées par le traitement ;
- la durée de conservation des données traitées ;
- le ou les service(s) chargé (s) de mettre en œuvre le traitement ainsi que les catégories de personnes qui, en raison de leurs fonctions ou pour les besoins du service, ont directement accès aux données collectées ;
- les destinataires habilités à recevoir communication des données traitées ;
- la fonction de la personne ou le service auprès duquel s'exerce le droit d'accès ;
- les dispositions prises pour assurer la sécurité des traitements, la protection et la confidentialité des données traitées ;
- l'indication du recours à un sous-traitant ou du transfert des données à caractère personnel à destination d'un pays tiers.

En cas de changement intervenu dans les mentions énumérées ci-dessus, le responsable du traitement en informe, sans délai, la HAPDP.

Les conditions de présentation de la demande d'autorisation et les procédures d'octroi des autorisations sont fixées par décret pris en Conseil des Ministres.

La HAPDP peut, par décision, exiger des conditions complémentaires de présentation de la demande d'autorisation ou de déclaration et des procédures d'octroi des autorisations.

La déclaration ou la demande d'autorisation peut être adressée à la HAPDP par voie électronique, postale ou par tout autre moyen contre remise d'un accusé de réception.

Article 31 : Règles spécifiques aux Formalités de demande d'autorisation

Sont soumis à l'autorisation préalable de la HAPDP avant toute mise en œuvre :

- le traitement des données à caractère personnel portant sur des données génétiques, médicales et sur la recherche scientifique dans ces domaines ;
- le traitement des données à caractère personnel portant sur des données relatives aux infractions, aux condamnations ou aux mesures de sûreté prononcées par les juridictions ;
- le traitement permettant l'interconnexion de fichiers de données à caractère personnel ;
- le traitement portant sur des identifiants uniques ou tout identifiant de portée générale, notamment le traitement portant sur un numéro d'identification national ou un numéro de téléphone ;
- le traitement des données à caractère personnel comportant des données biométriques ;
- le traitement des données à caractère personnel à des fins historiques, statistiques, démographiques et scientifiques, à condition qu'un motif d'intérêt public soit justifié ;
- le traitement portant transfert de données à caractère personnel à destination d'un pays tiers ;
- le traitement permettant le profilage ou l'analyse comportementale portant sur des données à caractère personnel ;
- le traitement de données à caractère personnel qui révèle les convictions ou activités religieuses, philosophiques, politiques, syndicales, ethniques, la vie sexuelle, la race, les mœurs, les mesures d'ordre social, les poursuites, les sanctions pénales ou administratives.

La demande d'autorisation est présentée par le Responsable du Traitement ou son représentant légal. L'autorisation ne l'exonère pas de sa responsabilité à l'égard des tiers.

Article 32 : Règles spécifiques aux Formalités de déclarations

Pour les catégories les plus courantes de traitement des données à caractère personnel, notamment celles dont la mise en œuvre n'est pas susceptible de porter atteinte à la vie privée ou sur les libertés, la HAPDP établit et publie des normes et procédures destinées à simplifier ou à exonérer le responsable du traitement de l'obligation de déclaration préalable. Dans ce cas, une déclaration simplifiée de conformité suffit selon le contenu adopté par la HAPDP.

Sauf décision particulière de la HAPDP, le récépissé de la déclaration simplifiée est délivré sans délai.

Dès réception de ce récépissé, le demandeur peut mettre en œuvre le traitement de données à caractère personnel.

Toutefois, il n'est exonéré d'aucune de ses responsabilités prévues par la présente loi.

Article 33 : Règles spécifiques aux Formalités de demande d'avis

Les opérations de traitement de données à caractère personnel opérées pour le compte de l'État, d'un établissement public ou d'une collectivité territoriale ou d'une personne morale de droit privé gérant un service public, sont décidées selon le cas, par acte législatif ou réglementaire, pris après avis motivé de la HAPDP.

Ces traitements sont relatifs :

- à la sûreté de l'État, à la défense ou à la sécurité publique ;
- à la prévention, à la recherche, à la constatation ou à la poursuite d'infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté ;
- au recensement général de la population ;
- au traitement de salaires, pensions, impôts, taxes et autres liquidations ;
- aux traitements des données qui révèlent les convictions ou les activités religieuses, philosophiques, politiques, syndicales, ethniques, la vie sexuelle, la race, la santé, les mœurs, les données génétiques ou biométriques, les mesures d'ordre social, les poursuites et les sanctions pénales ou administratives.

Article 34 : Règles spécifiques aux demandes d'avis consultatif

Les organismes publics ou privés et les personnes concernées peuvent saisir la HAPDP pour un avis consultatif sur toute question qui relève de la protection des données à caractère personnel dans les conditions fixées à l'article 30 de la présente loi.

Les autorités judiciaires peuvent également saisir la HAPDP d'une demande d'avis sur des éléments soumis à leur appréciation lors des contentieux relatifs à la protection des données à caractère personnel dans les conditions fixées par voie règlementaire.

Article 35 : Règles spécifiques à la saisine de la HAPDP pour la mise en conformité

Les déclarations, les demandes d'autorisation ou d'avis peuvent être adressées à la HAPDP par voie électronique, postale ou par tout autre moyen laissant traces écrites contre remise d'un accusé de réception.

La HAPDP se saisit d'office de tout traitement de données à caractère personnel mis en œuvre en violation des dispositions de la présente loi et de celles des autres textes législatifs et réglementaires contenant des dispositions relatives à la protection des données à caractère personnel.

La HAPDP peut aussi être saisie par toute personne physique ou morale.

Article 36 : Règles spécifiques au délai de traitement

LA HAPDP se prononce dans un délai d'un (1) mois à compter du dernier acte d'instruction notifié au demandeur pour les demandes d'autorisation ou d'avis et à compter du dépôt du dossier complet pour les déclarations.

Toutefois, ce délai peut être prorogé d'un délai supplémentaire sur décision motivée du Président de la Haute autorité. La décision de prorogation doit être notifiée au responsable du traitement.

L'absence de réponse de la HAPDP dans les délais précités équivaut à l'acceptation de la déclaration ou de la demande d'autorisation.

En cas d'urgence, le délai imparti à la HAPDP pour répondre à une demande d'avis est ramené à quinze (15) jours à la demande du gouvernement ou du parlement.

CHAPITRE VI : DES PRINCIPES DIRECTEURS DU TRAITEMENT DES DONNEES A CARACTERE PERSONNEL

Article 37 : Principe de légitimité du traitement

Le traitement des données à caractère personnel est considéré comme légitime si la personne concernée donne expressément son consentement préalable.

Toutefois, il peut être dérogé à cette exigence du consentement préalable lorsque le responsable du traitement est dûment autorisé et que le traitement est nécessaire :

- soit au respect d'une obligation légale à laquelle le responsable du traitement est soumis ;

- soit à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées ;
- soit à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à sa demande ;
- soit à la sauvegarde de l'intérêt ou des droits et libertés fondamentaux de la personne concernée.

Article 38 : Principes de finalité et de conservation

Les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes et ne peuvent être traitées ultérieurement de manière incompatible avec ces finalités.

Elles doivent être conservées pendant une durée qui n'excède pas la période nécessaire aux finalités pour lesquelles elles ont été collectées ou traitées ; au-delà de cette période requise, les données ne peuvent faire l'objet d'une conservation qu'en vue de répondre spécifiquement à un traitement à des fins historiques, statistiques ou de recherches en vertu des dispositions légales.

Article 39 : Principe de proportionnalité et d'exactitude

Les données collectées doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et traitées ultérieurement.

Elles doivent être exactes et, si nécessaire, mises à jour. Toute mesure raisonnable doit être prise pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont collectées et traitées ultérieurement, soient effacées ou rectifiées.

Article 40 : Principe de transparence, de licéité et de loyauté

Le principe de transparence implique une information obligatoire et claire de la part du responsable du traitement portant sur les données à caractère personnel.

La collecte, l'enregistrement, le traitement, le stockage et la transmission des données à caractère personnel doivent se faire de manière licite, loyale et non frauduleuse.

Article 41 : Principe de confidentialité et de sécurité

Les données à caractère personnel doivent être traitées de manière confidentielle et être protégées, notamment lorsque le traitement de ces données comporte des transmissions de données dans un réseau.

Lorsque le traitement est mis en œuvre pour le compte du responsable du traitement, celui-ci doit choisir un sous-traitant qui apporte des garanties suffisantes de sécurité et de

confidentialité. Il incombe au responsable du traitement ainsi qu'au sous-traitant de veiller au respect de ces mesures.

CHAPITRE VII : PRINCIPES SPECIFIQUES A CERTAINS TRAITEMENTS DE DONNEES A CARACTERE PERSONNEL

Article 42 : Traitement de données sensibles

Le traitement des données qui révèlent l'origine raciale, ethnique ou régionale, la filiation, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, la vie sexuelle, la santé et les mœurs, les données génétiques et biométriques, les mesures d'ordre social, les sanctions pénales ou administratives, est interdit, sauf, notamment, dans les cas suivants :

- lorsque le traitement porte sur des données manifestement rendues publiques par la personne concernée ;
- lorsque le traitement des données génétiques ou relatives à l'état de santé est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement ;
- lorsque le traitement, notamment des données génétiques, est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice de la personne concernée ;
- lorsque la personne concernée a donné son consentement par écrit, quel que soit le support, à un tel traitement et en conformité avec les textes en vigueur ;
- lorsque le traitement est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice dans le cadre d'une procédure judiciaire ou d'une enquête pénale. Dans ce cas, le traitement des données à caractère personnel n'est poursuivi que pour la constatation des faits ou pour la manifestation de la vérité ;
- lorsque le traitement est effectué dans le cadre des activités légitimes d'une fondation, d'une association ou de tout autre organisme à but non lucratif et apolitique, philosophique, religieuse, mutualiste ou syndicale. Dans ce cas, le traitement doit se rapporter aux seuls membres de cet organisme ou aux personnes entretenant avec celui-ci des contacts réguliers liés à sa finalité et que les données ne soient pas communiquées à des tiers sans le consentement des personnes concernées.

Article 43 : Traitements portant sur des données de santé

Les données de santé peuvent être collectées et traitées lorsque le traitement est nécessaire :

- aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements, ou de gestion de services de santé par les professionnels de santé et du secteur social et médico-social, dans les conditions prévues par la présente loi ;
- pour des motifs de santé publique, tels que la protection contre les risques sanitaires, ainsi que pour l'action humanitaire ;

- aux fins de sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne lorsque le consentement ne peut être recueilli ;
- pour des motifs d'intérêt public dans le domaine de la gestion des demandes de prestations et de services de protection sociale, de l'assistance et de l'assurance maladie dans les conditions prévues par la présente loi ;
- pour des motifs nécessaires à la constatation, à l'exercice ou à la défense d'un droit en justice ;
- à des fins de recherche après avis conforme du Comité National d'éthique pour la recherche en santé.

Le traitement de données de santé ne peut être mis en œuvre que par des médecins ou des personnes soumises, en raison de leurs fonctions, à l'obligation de garder le secret professionnel.

La HAPDP adopte, si nécessaire, des mesures ou des lignes directrices aux fins de préciser les modalités pratiques de traitement de certaines données de santé.

Article 44 : Echange et Partage de données de santé

L'échange et le partage de données de santé entre professionnels de santé doivent être limités aux informations strictement nécessaires à la coordination ou à la continuité des soins, à la prévention ou au suivi médico-social et social de la personne concernée.

Chaque professionnel de santé ne peut, dans ce cas, transmettre ou recevoir que les données qui relèvent du périmètre de ses missions en fonction de ses habilitations.

Article 45 : Communication des données de santé aux autres acteurs

Les données de santé peuvent être communiquées à des destinataires autorisés par un texte législatif ou réglementaire.

Les compagnies d'assurances et les employeurs ne peuvent pas être considérés comme des destinataires autorisés à accéder aux données relatives à la santé des personnes, sauf si un texte législatif ou règlementaire le prévoit, sous réserve des garanties appropriées et conformément aux principes directeurs visés au chapitre VI de la présente loi.

Article 46 : Traitement des données de santé à des fins de recherche médicale

Le traitement des données de santé à des fins de recherche médicale n'est autorisé que si la personne concernée y a consenti et que ses droits et libertés fondamentaux sont respectés.

La nécessité du traitement de données à des fins de recherche médicale doit être appréciée au regard de la finalité poursuivie par le projet de recherche et du risque encouru par la personne concernée.

La personne concernée doit disposer d'une information préalable, transparente, compréhensible et aussi précise que possible, concernant :

- la nature de la recherche envisagée, les choix éventuels qu'elle peut exercer ainsi que toutes conditions pertinentes régissant l'utilisation de ses données, y compris la reprise de contact et le retour d'informations ;
- les conditions applicables à la conservation des données, y compris les politiques en matière d'accès et éventuellement de communications ;
- les droits et garanties prévus par la loi et, notamment, son droit de refuser de participer à la recherche ainsi que de se retirer à tout moment.

Article 47 : Anonymisation des données de santé

Les données de santé doivent être anonymisées avant partage ou communication. Il en est de même pour les travaux de recherche. La présentation des résultats de recherche ne doit, en aucun cas, permettre l'identification ultérieure directe ou indirecte des personnes concernées.

Les données de santé permettant l'identification directe ou indirecte des personnes physiques doivent être hébergées sur le territoire national.

Les données individuelles transmises ne peuvent être conservées sous une forme permettant l'identification directe ou indirecte des personnes concernées au delà de la durée nécessaire à la recherche, sauf autorisation motivée de la HAPDP après avis du Comité National d'éthique pour la recherche en santé.

Article 48 : Traitement des données génétiques

Les données génétiques ne peuvent être traitées que dans les cas suivants :

- pour vérifier l'existence d'un lien génétique dans le cadre de l'administration de la preuve en justice ;
- pour l'identification d'une personne à l'occasion de la prévention ou la répression d'une infraction pénale déterminée ;
- à des fins de prévention, de diagnostic, ou à des fins thérapeutiques à l'égard de la personne concernée ou d'un membre de sa famille biologique, ou pour la recherche scientifique.

Sauf disposition législative ou réglementaire contraire, les données génétiques ne doivent être collectées et traitées que sous réserve du consentement de la personne concernée ou de son représentant légal.

Article 49 : Traitement de données biométriques

Le traitement de données biométriques doit répondre à une nécessité particulière, justifiée, et être entouré de garanties conformément aux dispositions de la présente loi.

Tout traitement portant sur des données biométriques doit faire l'objet d'une autorisation préalable de la HAPDP avant sa mise en œuvre.

Article 50 : Traitements de données relatives aux infractions, aux condamnations et aux mesures de sûreté

Seuls peuvent procéder aux traitements de données à caractère personnel relatives aux infractions, aux condamnations et aux mesures de sûreté :

- les juridictions et les autorités publiques agissant dans le cadre de leurs attributions légales ;
- les auxiliaires de justice, pour les stricts besoins de l'exercice des missions qui leur sont confiées.

Toute utilisation des données à caractère personnel pour des finalités judiciaires et policières autres que celles pour lesquelles elles ont été collectées doit être conforme aux dispositions prévues par la présente loi.

Article 51 : Traitement aux fins de prospection directe

Est interdite toute opération de prospection, quelle qu'en soit la nature, à l'aide de tout moyen de communication utilisant, sous quelque forme que ce soit, des données à caractère personnel d'une personne physique qui n'a pas exprimé son consentement préalable à recevoir de telles prospections.

Toute personne a le droit d'être informée, avant que des données la concernant ne soient utilisées pour la première fois, communiquées à des tiers ou utilisées pour le compte de tiers à des fins de prospections directes.

Article 52 : Décision individuelle basée sur le traitement automatisé

Aucune décision de justice, impliquant une appréciation sur le comportement d'une personne physique, ne peut avoir pour fondement un traitement automatisé des données à caractère personnel destiné à évaluer certains aspects de sa personnalité.

Aucune décision administrative ou privée, impliquant une appréciation sur un comportement humain, ne peut avoir pour seul fondement un traitement automatisé des données à caractère personnel donnant une définition du profil ou de la personnalité de l'intéressé.

Toute personne a le droit de connaître et de contester les informations et les raisonnements utilisés dans les traitements automatisés ou non, dont les résultats lui sont opposés.

Lorsque ce traitement relève de l'intelligence artificielle, les critères et la nature des données à caractère personnel fondant ce traitement lui sont indiqués dès la collecte.

Toutefois, une décision individuelle automatisée est admise si elle est :

- fondée sur le consentement explicite de la personne concernée ;
- nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et un responsable du traitement ;
- autorisée par une disposition législative ou réglementaire contraire.

Article 53 : Traitement aux fins de l'interconnexion des données

L'interconnexion des fichiers n'est autorisée par la HAPDP que si elle permet d'atteindre des objectifs légaux ou statutaires présentant un intérêt légitime pour les responsables des traitements.

Elle ne peut entraîner de discrimination ou de réduction des droits, des libertés et des garanties pour les personnes concernées, ni être assortie de mesures de sécurité inappropriées et doit tenir compte du principe de pertinence des données faisant l'objet de l'interconnexion.

Article 54 : Traitement des données sur les migrants

Tout système d'information et d'analyse des données à caractère personnel relatives aux migrants ne doit avoir pour finalités que la collecte, le traitement, le stockage, l'accessibilité, la diffusion, l'analyse des informations sur les migrants et leur partage éventuel.

La HAPDP adopte, si nécessaire, des mesures ou des lignes directrices aux fins de préciser les modalités pratiques de traitement de certaines données à caractère personnel relatives à la migration.

Article 55 : Traitement des données des personnes victimes de disparition forcée

La HAPDP adopte, si nécessaire, des mesures ou des lignes directrices aux fins de préciser les modalités pratiques de traitement de certaines données à caractère personnel relatives aux personnes victimes de disparition forcée.

Article 56 : Traitement portant sur des méga données

Tout Responsable du traitement portant sur des méga-données permettant l'identification ou la ré-identification d'une personne physique est astreint au respect des dispositions de la présente loi, notamment le principe du consentement, de transparence et de finalité.

Le responsable de traitement portant sur des mégas données doit procéder en particulier à l'examen préalable de l'impact potentiel dudit traitement sur les droits et libertés fondamentaux des personnes afin :

- d'identifier et d'évaluer les risques de chaque traitement et de ses incidences potentiellement négatives sur les droits et libertés fondamentaux des personnes, en particulier, le droit à la protection des données à caractère personnel et le droit à la non-discrimination, en tenant compte des impacts sociaux et éthiques ;
- de prévoir des mesures de sécurité appropriées, notamment dès la conception pour atténuer les risques éventuels ;
- de réévaluer régulièrement le risque de ré-identification eu égard aux avancées technologiques relatives aux techniques d'anonymisation.

Article 57 : Traitement portant sur l'intelligence artificielle

L'intelligence artificielle s'entend comme l'ensemble de sciences, de théories et de techniques dont le but est de reproduire par une machine des capacités cognitives d'un être humain.

Les développeurs, fabricants et fournisseurs de services en Intelligence Artificielle doivent respecter les dispositions de la présente loi.

L'obligation déclarative auprès de la HAPDP s'impose aux développeurs, aux fabricants et aux prestataires de services opérant à partir du territoire national.

Article 58 : Traitement relatif à l'internet des objets

Les développeurs, fabricants et prestataires de services des objets connectés à Internet sont tenus de respecter les dispositions de la présente loi, notamment le droit à l'information sur les risques encourus et les mesures techniques appropriées mises en œuvre.

Article 59 : Traitement portant sur des données ouvertes (open data)

Les autorités publiques et les organismes privés exécutant une mission de service public peuvent procéder à la communication et à l'ouverture des données publiques comportant des données à caractère personnel, à condition de concilier le droit d'accès du public aux documents officiels et le droit à la protection des données à caractère personnel.

Article 60 : Conditions de réutilisation des données ouvertes

Les informations publiques ou les documents administratifs comportant des données à caractère personnel peuvent faire l'objet d'une réutilisation à condition que :

- la loi le prévoit ;
- la personne concernée ait donné expressément son consentement ;
- l'autorité publique ou l'organisme privé exécutant une mission de service public soit en mesure de les rendre anonymes de manière irréversible.

Article 61 : Traitement relatif aux systèmes de vidéosurveillance et télésurveillance

Sous réserve de la législation en vigueur, les dispositifs de vidéosurveillance et de télésurveillance, en dehors des domiciles privés, doivent faire l'objet avant leur installation d'une formalité déclarative auprès de la HAPDP.

Les dispositifs de vidéosurveillance et de télésurveillance ne peuvent être utilisés que s'ils sont nécessaires pour assurer la sécurité des biens et des personnes.

Ils peuvent être utilisés, notamment dans les lieux suivants :

- les lieux ouverts au public et leurs entrées ;

- les parkings, les moyens de transport public, les stations et les aéroports ;
- les lieux de travail.

Toutefois, l'installation de caméras de surveillance sur les lieux de travail et dans les domiciles privés ne peut avoir pour but la surveillance délibérée, systématique et permanente des employés et du voisinage.

Le public doit être informé d'une manière claire et permanente de l'existence de moyens de vidéosurveillance ou de télésurveillance.

Une affiche suffisamment visible doit signaler la présence du système, la référence du récépissé délivré par la HAPDP ainsi que les coordonnées du service chargé de répondre à l'exercice des droits d'accès, d'opposition et de suppression.

La HAPDP adopte des mesures et des lignes directrices aux fins de préciser les conditions de mise en place des dispositifs de vidéosurveillance et de télésurveillance.

Article 62 : Traitement portant transfert des données vers un État assurant un niveau de protection suffisant

Le responsable d'un traitement ne peut transférer des données à caractère personnel vers un autre État que si cet État assure un niveau de protection suffisant de la vie privée, des droits et libertés fondamentaux des personnes concernées.

Avant tout transfert des données à caractère personnel vers un autre Etat, le responsable de traitement, doit au préalable :

- mettre en œuvre des mesures de sécurité techniques et organisationnelles garantissant notamment le chiffrement, la disponibilité, la confidentialité, l'intégrité des données, ainsi que la résilience constante des systèmes et des services de traitements ;
- requérir l'autorisation de la HAPDP.

Le caractère suffisant du niveau de protection assuré par un État s'apprécie en fonction notamment des dispositions législatives et réglementaires en vigueur dans cet État en matière de protection de données personnelles et l'existence d'une autorité de protection.

Le niveau adéquat de la protection des données à caractère personnel peut aussi être apprécié par :

- les conventions ou accords internationaux auxquels l'Etat est partie ;
- les garanties appropriées agréées par la HAPDP.

À tout moment, la HAPDP peut retirer son autorisation, dès lors que des circonstances exceptionnelles surviennent dans le pays destinataire.

Article 63 : Traitement portant transfert des données vers un État n'assurant pas un niveau de protection suffisant.

Nonobstant les dispositions de l'article 62 ci-dessus, un transfert de données à caractère personnel vers un pays n'assurant pas un niveau adéquat de protection peut être effectué dans les conditions suivantes :

- lorsque la personne concernée a donné son consentement spécifique, libre, éclairé et non équivoque, après avoir été informée des risques liés à l'absence de garanties appropriées ;
- lorsque le transfert est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée et à la sauvegarde de l'intérêt public ;
- lorsque le transfert est autorisé par un texte législatif ou réglementaire, après avis de la HAPDP, notamment dans le cadre de l'exécution d'une mesure d'entraide judiciaire internationale ;
- lorsque le traitement s'effectue en application d'un accord bilatéral ou multilatéral auquel le Niger est partie ;
- lorsqu'un contrat homologué par la HAPDP liant le responsable du traitement et ses cocontractants prévoit des clauses contractuelles ou des règles internes qui garantissent un niveau adéquat de protection de la vie privée ainsi que les droits et libertés fondamentaux des personnes ;
- lorsque le transfert permet d'assurer la constatation, l'exercice ou la défense d'un droit en justice ;
- lorsque le transfert permet la conclusion ou l'exécution d'un contrat, dans l'intérêt de la personne concernée, entre le responsable du traitement et un tiers.

CHAPITRE VIII : DES OUTILS DE CONFORMITE

Article 64 : Registre des opérations de traitement

Tout responsable du traitement et tout sous-traitant doivent tenir préalablement à la mise en œuvre d'un traitement un registre des opérations qui consigne la collecte, la modification, la consultation, la communication, y compris les transferts, l'interconnexion et la suppression de données à caractère personnel.

Le responsable du traitement et le sous-traitant mettent ce registre des opérations de traitement à la disposition de la HAPDP, lorsqu'elle en fait la demande, notamment lors d'un contrôle sur place ou sur pièces.

La HAPDP établit un modèle de registre des opérations de traitement destiné aux responsables du traitement et aux sous-traitants.

Article 65 : Certificat de conformité

La HAPDP délivre des certificats de conformité pour les procédures ou les produits relatifs à la protection des données à caractère personnel, lorsque ceux-ci sont conformes à des référentiels.

Elle élabore et publie des référentiels de certificat de conformité portant sur des formations, des procédures, des produits ou des outils de conformité.

Article 66 : Homologation des politiques de protection

La HAPDP homologue les politiques de protection des données à caractère personnel présentées par les responsables de traitement ou les sous-traitants. L'homologation porte notamment sur les codes de conduite, les chartes, les règles contraignantes d'entreprise ou tout document relatif à des mesures de protection des données à caractère personnel.

L'homologation de politiques de protection des données personnelles est soumise à la HAPDP sous forme de demande d'avis.

Article 67 : Analyse d'impact

Pour certains traitements portant sur des données sensibles susceptibles de porter atteinte aux droits et liberté des personnes physiques, la HAPDP peut, avant délivrance d'une autorisation, exiger du responsable du traitement une analyse d'impact sur la vie privée des personnes concernées.

La HAPDP établit et publie la liste des opérations de traitement qui sont susceptibles de présenter un risque élevé sur les droits et libertés des personnes concernées et qui nécessitent une analyse d'impact.

Elle adopte des mesures et des lignes directrices aux fins de préciser les conditions et procédures de réalisation de cette analyse d'impact.

CHAPITRE IX : DES DROITS DES PERSONNES CONCERNEES

Article 68 : Droit à l'information

Sauf disposition législative ou réglementaire contraire, le Responsable d'un traitement est tenu de fournir à la personne concernée les informations sur ledit traitement, au plus tard, lors de la collecte.

Article 69 : Droit d'accès direct

Les personnes concernées par un traitement ont un droit d'accès direct à leurs données. Ce droit d'accès peut, selon leur choix, s'exercer par consultation sur place et/ou par délivrance de copie.

Toute personne physique dont les données font l'objet d'un traitement peut demander sous forme de questions et obtenir du responsable du traitement, les informations la concernant.

En cas d'impossibilité d'accès pour la personne concernée, le droit d'accès peut être exercé par la HAPDP qui dispose d'un pouvoir d'investigation en la matière et qui peut ordonner la rectification, l'effacement ou le verrouillage des données dont le traitement n'est pas conforme à la présente loi.

La HAPDP communique à la personne concernée le résultat de ses investigations.

En cas d'exercice du droit d'accès, une copie des données est délivrée à la personne concernée à sa demande. Le responsable du traitement peut subordonner la délivrance de cette copie au paiement d'une somme qui ne peut excéder le coût de la reproduction.

En cas de risque de dissimulation ou de disparition des données, la personne concernée peut en informer la HAPDP qui prend toute mesure de nature à éviter cette dissimulation ou cette disparition.

Toute personne qui dans l'exercice de son droit d'accès a des raisons sérieuses d'admettre que les données qui lui ont été communiquées ne sont pas conformes aux données traitées, peut en informer la HAPDP qui procède aux vérifications nécessaires.

Le responsable du traitement peut s'opposer aux demandes manifestement abusives, notamment par leur nombre, leur caractère répétitif ou systématique.

En cas de contestation, la charge de la preuve du caractère manifestement abusif des demandes incombe au responsable du traitement à qui elles sont adressées.

Article 70 : Droit d'accès indirect

Par dérogation à l'article 68 ci-dessus, lorsqu'un traitement intéresse la sûreté de l'État, la défense ou la sécurité publique, le droit d'accès s'exerce dans les conditions suivantes :

- la demande est adressée à la HAPDP qui désigne un de ses membres pour mener les investigations nécessaires. Celui-ci peut se faire assister d'un autre agent de la HAPDP. Il est notifié au requérant qu'il a été procédé aux vérifications ;
- lorsque la HAPDP constate, en accord avec le responsable du traitement, que la communication des données qui y sont contenues ne met pas en cause les finalités du traitement, la sûreté de l'État, la défense ou la sécurité publique, ces données peuvent être communiquées au requérant ;
- lorsque le traitement est susceptible de comporter des informations dont la communication ne mettrait pas en cause les finalités qui lui sont assignées, l'acte réglementaire portant création du fichier peut prévoir que ces informations peuvent être communiquées au requérant par le gestionnaire du fichier directement saisi.

Article 71 : Droit de rectification

Toute personne physique, justifiant de son identité, peut exiger du responsable d'un traitement que soient, selon les cas, rectifiées, complétées, mises à jour, verrouillées ou effacées, les données la concernant, qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite.

Les ayants droit d'une personne décédée, justifiant de leur identité peuvent, si des éléments portés à leur connaissance leur laissent présumer que les données la concernant, faisant l'objet d'un traitement n'ont pas été actualisées, exiger du responsable de ce traitement qu'il

prenne en considération le décès et procède, dans un délai d'un (1) mois après l'enregistrement de la demande, aux mises à jour nécessaires.

Lorsque les ayants droit en font la demande, le responsable du traitement doit justifier, sans frais pour le demandeur, qu'il a procédé aux opérations exigées en vertu de l'alinéa précédent.

Article 72 : Droit d'opposition

Toute personne physique concernée a le droit de :

- s'opposer, pour des motifs légitimes tenant à sa situation particulière, à ce que des données la concernant fassent l'objet d'un traitement, sauf dispositions légales prévoyant expressément le traitement. Dans ce cas, le traitement mis en œuvre par le responsable du traitement ne peut porter sur les données en cause ;
- s'opposer et sans frais, au traitement des données la concernant à des fins de prospection ;
- être informée avant que des données la concernant ne soient pour la première fois communiquées à des tiers ou utilisées pour le compte de tiers à des fins de prospection et de se voir, expressément accorder le droit de s'opposer, sans frais, à ladite communication ou utilisation.

Les dispositions du premier alinéa du présent article ne s'appliquent pas lorsque le traitement répond à une obligation légale ou si le responsable du traitement démontre à la HAPDP l'existence de motifs légitimes justifiant le traitement qui prévalent sur les intérêts, les droits et libertés fondamentaux de la personne concernée.

Article 73 : Droit de suppression

Toute personne physique justifiant de son identité peut exiger du responsable d'un traitement que les données la concernant, qui sont inexactes, incomplètes, équivoques, périmées ou dont la collecte, l'utilisation, la communication ou la conservation est interdite soient supprimées.

Le droit de suppression peut s'exercer pour l'un des motifs suivants :

- absence du consentement de la personne concernée ou exercice du droit de retrait dudit consentement sauf disposition législative ou réglementaire contraire ;
- disparition de la ou des finalité(s) servant de fondement au traitement ;
- traitement illicite des données collectées ;
- suppression des données en vertu d'une disposition législative ou réglementaire ;
- traitement de données concernant un mineur.

Toutefois, le droit de suppression ne peut s'exercer lorsque la conservation des données à caractère personnel est nécessaire :

- soit en vertu d'un motif prévu par une disposition législative ou réglementaire ;
- soit à l'exercice du droit à la liberté d'expression ;

- soit pour des motifs d'intérêt général dans le domaine de la santé publique, de la recherche scientifique ou à des fins statistiques ou archivistiques ;
- soit en vertu d'une obligation légale de conserver les données ;
- soit en vertu d'une disposition législative ou réglementaire visant la constatation, l'exercice ou la défense des droits à la justice.

La personne concernée a le droit d'obtenir du responsable du traitement l'effacement de données la concernant et la cessation de la diffusion de ces données, en particulier en ce qui concerne des données à caractère personnel que la personne concernée avait rendues disponibles lorsqu'elle était mineure, ou pour l'un des motifs suivants :

- les données ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées ;
- la personne concernée a retiré le consentement sur lequel est fondé le traitement ou lorsque le délai de conservation autorisé a expiré et qu'il n'existe pas d'autre motif légal au traitement des données ;
- la personne concernée s'oppose au traitement des données la concernant lorsqu'il n'existe pas de motif légal audit traitement ;
- le traitement des données n'est pas conforme aux dispositions de la présente loi ;
- pour tout autre motif légitime.

Si les données ont été transmises à un tiers, le responsable du traitement doit accomplir les diligences utiles afin de lui notifier les opérations qu'il a effectuées conformément au premier alinéa, et celles que le tiers doit effectuer.

Lorsque l'intéressé en fait la demande par écrit, quel que soit le support, le responsable du traitement doit justifier, sans frais pour le demandeur, qu'il a procédé aux opérations exigées en vertu des alinéas précédents dans un délai d'un (1) mois après l'enregistrement de la demande.

En cas de contestation, la charge de la preuve incombe au responsable du traitement auprès duquel est exercé le droit d'opposition.

Article 74 : Droit à l'oubli numérique

Le droit à l'oubli numérique est la faculté reconnue à la personne concernée d'obtenir du responsable du traitement, le retrait de données à caractère personnel relatives à sa vie privée, à des activités passées, rendues publiques sur un site web, accessible ou non par un moteur de recherche.

La personne concernée dispose d'un droit à l'oubli numérique concernant ses données à caractère personnel qui sont collectées et rendues publiques.

Lorsque le responsable du traitement a rendu public les données à caractère personnel de la personne concernée, il prend toutes les mesures raisonnables, y compris les mesures techniques, en ce qui concerne les données publiées sous sa responsabilité, en vue d'informer

les tiers qui traitent lesdites données qu'une personne concernée leur demande d'effacer tous liens vers ces données, ou toute copie ou reproduction de celles-ci.

Lorsque le responsable du traitement a autorisé un tiers de publier des données à caractère personnel, il est réputé responsable de cette publication et prend toutes les mesures appropriées pour mettre en œuvre le droit à l'oubli numérique et à l'effacement de ces données.

Le responsable du traitement met en place des mécanismes appropriés assurant la mise en œuvre du respect du droit à l'oubli numérique et à l'effacement des données à caractère personnel ou examine périodiquement la nécessité de conserver ces données, conformément aux dispositions de la présente loi.

Lorsque l'effacement est effectué, le responsable du traitement ne procède à aucun autre traitement de ces données.

La HAPDP adopte des mesures et des lignes directrices aux fins de préciser :

- les conditions de la suppression des liens vers ces données, des copies ou des reproductions de celles-ci existant dans les services de communication électronique accessibles au public ;
- les conditions et les critères applicables à la limitation du traitement des données à caractère personnel.

Article 75 : Droit à la limitation du traitement

L'exercice du droit à la limitation du traitement permet à toute personne de demander à un organisme de geler temporairement l'utilisation de certaines de ses données.

Les modalités de mise en œuvre du droit à la limitation du traitement sont fixées par décret pris en Conseil des Ministres.

Article 76 : Droit à la portabilité des données

Toute personne physique, justifiant de son identité, a le droit de transmettre ses données à un autre responsable du traitement, selon l'état de la technologie, sans que le responsable du traitement auquel les données ont été communiquées ne s'y oppose. Le droit à la portabilité des données ne doit faire obstacle :

- ni aux droits et libertés des tiers ;
- ni à l'exécution d'une mission d'intérêt public ou à l'exercice de l'autorité publique par le responsable du traitement ;
- ni à l'exercice du droit de suppression.

Lorsque des données à caractère personnel font l'objet d'un traitement automatisé dans une forme structurée et couramment utilisée, la personne concernée a le droit d'obtenir auprès du responsable du traitement une copie des données faisant l'objet du traitement automatisé

dans un format électronique structuré qui est couramment utilisé, et qui permet la réutilisation de ces données par la personne concernée.

Lorsque la personne concernée a fourni les données à caractère personnel et que le traitement est fondé sur le consentement ou sur un contrat, elle a le droit de transmettre ces données et toutes informations qu'elle a fournies, et qui sont conservées par un système de traitement automatisé à un autre système dans un format électronique qui est couramment utilisé, sans que le responsable du traitement auquel les données à caractère personnel sont retirées n'y fasse obstacle.

La HAPDP peut préciser le format électronique, ainsi que les normes techniques, les modalités et les procédures pour la transmission de données à caractère personnel.

CHAPITRE X : DES OBLIGATIONS DES RESPONSABLES DES TRAITEMENTS ET DE LEURS SUBORDONNES

Article 77 : Obligations générales du responsable du traitement

En tenant compte de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer à la HAPDP que le traitement est effectué conformément aux dispositions de la présente loi.

A défaut, il engage sa responsabilité directe en cas de manquement aux dispositions de la présente loi.

Article 78 : Obligation conjointe des responsables du traitement

Lorsque deux responsables du traitement ou plus déterminent conjointement les finalités et les moyens du traitement, ils sont conjointement responsables de ce traitement.

Chaque responsable conjoint du traitement définit de manière transparente son rôle et sa relation vis-à-vis des personnes concernées aux fins d'assurer le respect des exigences de la présente loi.

Toute personne, concernée par un traitement avec plusieurs responsables conjoints, peut exercer les droits que lui confère la présente loi à l'égard de chacun des responsables du traitement.

Article 79 : Obligation de désigner un correspondant à la protection des données à caractère personnel.

Toute personne morale de droit privé, responsable d'un traitement portant sur des données à caractère personnel, doit désigner au sein de son organisme un correspondant à la protection des données à caractère personnel.

Le correspondant à la protection des données à caractère personnel est une personne physique ou morale bénéficiant de qualifications requises pour exercer de telles missions.

La désignation du correspondant par le responsable du traitement est notifiée à la HAPDP Elle est également portée, le cas échéant, à la connaissance des instances représentatives du personnel de l'organisme.

Les modalités de désignation, le profil et les garanties d'exercice de la fonction du correspondant à la protection des données ainsi que les obligations du responsable du traitement sont fixées par décret pris en Conseil des Ministres.

Les responsables du traitement relevant du secteur public doivent désigner un point focal qui fait office de correspondant.

Article 80 : Garanties et obligations du correspondant à la protection des données à caractère personnel

Le correspondant à la protection des données à caractère personnel ne peut faire l'objet d'aucune sanction de la part de l'employeur dans l'accomplissement de ses missions.

Il tient une liste des traitements effectués immédiatement accessible à toute personne concernée qui en fait la demande.

En cas de manquement constaté à ses devoirs, le correspondant est déchargé de ses fonctions sur demande de la HAPDP.

En outre le responsable du traitement peut décharger le correspondant de ses fonctions et le notifie à la HAPDP.

Article 81 : Obligations de confidentialité

Le traitement des données à caractère personnel est confidentiel. Tout traitement est effectué exclusivement par des personnes qui agissent selon leurs fonctions, sous l'autorité du responsable du traitement ou, le cas échéant, sous l'autorité du sous-traitant et seulement sur ses instructions.

Article 82 : Obligations de sécurité

Les responsables du traitement et les sous-traitants doivent mettre en œuvre des mesures techniques et organisationnelles visant à empêcher que les données à caractère personnel soient déformées, endommagées, ou que des tiers non autorisés y aient accès, compte tenu de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, pour les droits et libertés des personnes physiques.

Les mesures techniques pouvant être prises par le responsable du traitement afin de garantir un niveau de sécurité adapté au risque incluent :

- la pseudonymisation, le cryptage, l'anonymisation et le chiffrement des données à caractère personnel ;
- les moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
- la procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement ;
- la mise en œuvre de politiques de sécurité appropriées en matière de protection des données par le responsable du traitement et ses sous-traitants, notamment :
    - l'obligation de protection dès la conception, tant au moment de la détermination des moyens du traitement, qu'au moment de l'utilisation dudit traitement ;
    - l'obligation de protection par défaut consistant à garantir que seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées.

Article 83 : Obligations de notifier les failles de sécurité

Dès que le responsable du traitement apprend qu'une violation de données à caractère personnel s'est produite, il le notifie, en priorité à la HAPDP, sans délai après en avoir pris connaissance.

Le non-respect de cette disposition doit être justifié et motivé par le responsable du traitement auprès de la HAPDP.

Lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement communique la faille de sécurité à la personne concernée dans les meilleurs délais.

Le responsable du traitement n'est pas tenu à l'obligation de notification lorsqu'il est raisonnable de croire que la violation en question n'engendre pas de risque pour les droits et les libertés d'une personne physique.

Article 84 : Obligations de conservation

Les données à caractère personnel doivent être conservées pendant une durée qui n'excède pas la période nécessaire aux finalités pour lesquelles elles ont été collectées ou traitées.

Au delà de la durée nécessaire, les données à caractère personnel ne peuvent être conservées qu'en vue de leur traitement à des fins historiques, statistiques ou de recherche ou d'intérêt public et selon des garanties appropriées définies par la législation en vigueur ou, à défaut, par la HAPDP.

Article 85 : Obligations de pérennité

Le responsable du traitement est tenu de prendre toute mesure utile pour s'assurer que les données à caractère personnel traitées peuvent être exploitées quel que soit le support technique utilisé.

Article 86 : Obligations des sous-traitants

Lorsqu'un traitement est mis en œuvre pour le compte du responsable du traitement, celui-ci choisit un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements à effectuer. Il incombe au responsable du traitement ainsi qu'au sous-traitant de veiller au respect de ces mesures.

Les sous-traitants sont soumis aux mêmes obligations que les responsables du traitement.

Tout traitement effectué pour le compte du responsable du traitement par un sous-traitant doit être régi par un contrat de confidentialité ou tout autre acte juridique consigné par écrit qui lie les parties.

Le sous-traitant notifie au responsable du traitement toute violation de données à caractère personnel dans les meilleurs délais et au plus tard dans les 72 heures après en avoir pris connaissance.

CHAPITRE XI : DU CONTRÔLE DE CONFORMITE DES TRAITEMENTS

Article 87 : Agents de contrôle

Le Président de la HAPDP peut charger des agents pour procéder aux vérifications et investigations nécessaires au contrôle de la mise en œuvre des traitements de données à caractère personnel et du respect des délibérations de la HAPDP.

Les agents de contrôle de la HAPDP prêtent serment devant la Cour d'Appel de Niamey en ces termes : « ***Je jure de bien et loyalement remplir mes fonctions d'agent de contrôle de la Haute Autorité de Protection des Données à caractère Personnel en toute indépendance et impartialité, de garder le secret sur toute information ou tout fait dont j'aurai eu connaissance à l'occasion de l'exercice de mes fonctions*** ».

Article 88 : Mise en œuvre du contrôle

Dans le cadre de l'exercice de leur mission, les contrôleurs ont accès aux lieux, aux locaux, aux enceintes, aux installations ou aux établissements servant à la mise en œuvre d'un traitement des données à caractère personnel, à l'exclusion des parties de ceux-ci affectées au domicile privé.

Les modalités pratiques de mise en œuvre du contrôle sont précisées par délibération de la HAPDP.

CHAPITRE XII : DE LA COOPERATION

Article 89 : Principe

La HAPDP met en œuvre des procédures de coopération et d'assistance mutuelle avec les autorités de régulation des autres États et réalise avec elles des opérations conjointes dans des conditions fixées par un accord ou une Convention.

La HAPDP peut porter assistance à toute personne concernée à la demande d'une autorité de protection des données à caractère personnel d'un autre pays ou d'une autorité de protection instituée dans le cadre d'une organisation internationale.

Article 90 : Coopération entre Autorités de protection

La HAPDP crée les conditions de coopération avec les autres Autorités exerçant des compétences analogues au niveau régional et international, notamment en matière d'harmonisation des pratiques, de renforcement des capacités et de la promotion de la protection des données à caractère personnel.

Article 91 : Assistance et entraide mutuelle

La HAPDP met en œuvre toute mesure d'assistance et d'entraide mutuelle avec les autres Autorités de protection de données, notamment en matière de contrôle et des transferts transfrontaliers de données à caractère personnel.

CHAPITRE XIII : DES SANCTIONS ADMINISTRATIVES ET PECUNIAIRES

Article 92 : Mesures administratives

La HAPDP peut prononcer, après une procédure contradictoire, les mesures suivantes :

- un avertissement à l'égard du responsable du traitement ne respectant pas les obligations découlant de la présente loi ;
- une mise en demeure de faire cesser les manquements concernés dans le délai qu'elle fixe.

Si le responsable du traitement ne se conforme pas à la mise en demeure qui lui a été adressée, la HAPDP peut prononcer à son encontre, les sanctions suivantes :

- le retrait provisoire de l'autorisation accordée ;
- le retrait définitif de l'autorisation ;
- les sanctions pécuniaires.

Article 93 : Mesures conservatoires

Lorsque la mise en œuvre d'un traitement ou l'exploitation de données à caractère personnel persiste entrainant une violation de droits et libertés, la HAPDP peut, après procédure contradictoire, décider :

- de l'interruption de la mise en œuvre du traitement ;
- du verrouillage de certaines données traitées ;

- de l'interdiction temporaire ou définitive du traitement contraire aux dispositions de la présente loi.

Article 94 : Sanctions pécuniaires.

Le montant de la sanction pécuniaire est proportionnel à la gravité des manquements commis et aux avantages tirés de ce manquement.

Le montant de cette sanction ne peut excéder la somme de 100.000.000 de francs.

En cas de manquement réitéré dans les deux années à compter de la date à laquelle la sanction pécuniaire précédemment prononcée est devenue définitive, il ne peut excéder 200.000.000 de francs ou, s'agissant d'une entreprise, 5% du chiffre d'affaires hors taxes du dernier exercice clos dans la limite de 500.000.000 de francs.

Les sanctions pécuniaires prononcées par la HADPD sont appliquées sans préjudice de sanctions pénales prévues par la législation en vigueur.

CHAPITRE XIV : DES DISPOSITIONS PENALES

Article 95 : Traitement illicite des données sensibles

Est puni d'une peine d'emprisonnement de trois (3) mois à cinq (5) ans et d'une amende de 5.000.000 à 50.000.000 de francs , le fait, hors les cas prévus à l'article 42 de la présente loi, de procéder à la collecte et à tout traitement de données qui révèlent l'origine raciale, ethnique ou régionale, la filiation, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, la vie sexuelle ou l'orientation sexuelle, les données génétiques ou plus généralement celles relatives à l'état de santé de la personne concernée.

Article 96 : Prospection directe sans consentement préalable

Est punie d'une peine d'emprisonnement de trois (3) mois à trois (3) ans et d'une amende de un million (1.000.000) à dix millions (10.000.000) de francs, ou de l'une de ces deux peines seulement, la prospection directe à l'aide de tout moyen de communication utilisant, sous quelque forme que ce soit, les données à caractère personnel d'une personne physique qui n'a pas exprimé son consentement préalable à recevoir de telles prospections.

Article 97 : Entrave aux actions de la HAPDP

Est puni d'une peine d'emprisonnement de trois (3) mois à deux (2) ans et d'une amende de un million (1.000.000) à dix millions (10.000.000) de francs, ou de l'une de ces deux peines seulement, quiconque, personne physique, entrave l'action de la HAPDP :

- soit en s'opposant à l'exercice des missions confiées à ses membres ou à ses agents habilités, en application des dispositions de la présente loi ;

- soit en refusant de communiquer à ses membres ou aux agents habilités, les renseignements et documents utiles à leur mission, ou en dissimulant lesdits documents, ou en les faisant disparaître ;
- soit en communiquant des informations qui ne sont pas conformes au contenu des enregistrements tel qu'il était au moment où la demande a été formulée ou qui ne présentent pas ce contenu sous une forme directement accessible.

Le Procureur de la République territorialement compétent est informé, sans délai, et prend toutes les mesures appropriées en vue de poursuivre les auteurs, coauteurs ou complices.

Article 98 : Non-respect des mesures de sécurité

Est puni d'une peine d'emprisonnement de trois (3) mois à deux (2) ans et d'une amende de un million (1.000.000) à dix millions (10.000.000) de francs, ou de l'une de ces deux peines seulement, le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans prendre toutes les précautions utiles pour préserver la sécurité desdites données, notamment empêcher qu'elles soient déformées, endommagées ou communiquées à des tiers non autorisés.

Article 99 : Détournement de finalité

Est puni d'une peine d'emprisonnement de trois (3) mois à cinq (5) ans et d'une amende de cinq millions (5.000.000) à cinquante millions (50.000.000) de francs, ou de l'une de ces deux peines seulement, le fait de détourner la finalité d'une collecte, d'un traitement ou d'un transfert de données à caractère personnel vers un pays tiers en violation de la présente loi.

Article 100 : Communication non autorisée des données à caractère personnel

Est puni d'une peine d'emprisonnement de trois (3) mois à cinq (5) ans et d'une amende de cinq millions (5.000.000) à cinquante millions (50.000.000) de francs, ou de l'une de ces deux peines seulement, le fait de communiquer à des tiers non autorisés ou d'accéder intentionnellement sans autorisation ou de façon illicite à des fichiers contenant des données à caractère personnel.

Article 101 : Collecte frauduleuse, déloyale ou illicite de données

Est puni d'une peine d'emprisonnement de trois (3) mois à cinq (5) ans et d'une amende de cinq millions (5.000.000) à cinquante millions (50.000.000) de francs, ou de l'une de ces deux peines seulement, le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite.

Article 102 : Entraves à l'exercice des droits de la personne concernée

Est puni d'une peine d'emprisonnement de trois (3) mois à deux (2) ans et d'une amende de un million (1.000.000) à vingt millions (20.000.000) de franc, ou de l'une de ces deux peines seulement, le fait d'entraver sans raison légitime, l'exercice d'un droit consacré par la

présente loi lors d'un traitement de données à caractère personnel concernant une personne physique.

Article 103 : Conservation illicite de données

Est puni d'un emprisonnement de trois (3) mois à deux (2) ans et d'une amende de cinq millions (5.000.000) à cinquante millions (50.000.000) de francs, ou de l'une de ces deux peines seulement, quiconque conserve des données à caractère personnel sous forme identifiable directement ou indirectement au-delà de la durée prévue par la législation en vigueur ou celle prévue dans la délibération de la HAPDP autorisant le traitement ou par la déclaration préalable à la mise en œuvre de ce traitement.

Article 104 : Divulgation non autorisée de données à caractère personnel

Est puni d'une peine d'emprisonnement de trois (3) mois à cinq (5) ans et d'une amende de cinq millions (5.000.000) à cinquante millions (50.000.000) de francs, ou de l'une de ces deux peines seulement, le fait pour tout responsable du traitement, qui recueille, à l'occasion de leur enregistrement, de leur classement, de leur transmission ou d'une autre forme de traitement, des données à caractère personnel dont la divulgation aurait pour effet de porter atteinte à l'honneur et à la considération de la personne concernée ou à l'intimité de sa vie privée et les porte, sans son autorisation, à la connaissance d'un tiers qui n'a pas qualité pour les recevoir.

La divulgation prévue à l'alinéa précédent est sanctionnée d'une amende de cinq cent mille (500.000) à un million (1.000.000) de francs, lorsqu'elle a été commise par imprudence ou négligence.

Article 105 : Récidive

En cas de récidive, les dispositions prévues aux articles 59 à 61 du code pénal sont applicables.

Article 106 : Mesures complémentaires

La juridiction compétente peut en outre prononcer la confiscation de tous supports matériels des données à caractère personnel objet de la violation de la règlementation, tels que des fichiers manuels, disques et bandes magnétiques ou tout support de stockage, ou ordonner l'effacement de ces données.

La confiscation ou l'effacement peut être ordonné, même si les supports matériels des données à caractère personnel n'appartiennent pas à la personne sanctionnée.

Lorsque la juridiction compétente prononce une sanction au titre des articles 95 à 104 de la présente loi, elle peut en outre interdire au Responsable du Traitement condamné de gérer, personnellement ou par personne interposée et pour deux ans au maximum, tout traitement de données à caractère personnel.

Lorsque la juridiction compétente prononce une sanction au titre des articles 109 et suivants, des extraits sont publiés dans un ou plusieurs journaux d'annonces légales, dans les conditions qu'elle détermine, aux frais du condamné.

CHAPITRE XV : DES RECLAMATIONS, PLAINTES ET RECOURS

Article 107 : Réclamations auprès du Responsable de Traitement

La réclamation consiste pour toute personne physique, justifiant de son identité, ou les ayants droit d'une personne décédée à exiger du Responsable d'un Traitement que soient, selon les cas :

- respectés les droits d'accès, d'opposition et de rectification des données à caractère personnel la concernant, qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite ;

- complétées, mises à jour, verrouillées ou supprimées les données la concernant, qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite.

Article 108 : Plaintes auprès de la HAPDP

Toute personne qui se prétend lésée ou atteinte dans sa vie privée, par le traitement automatisé ou non des données à caractère personnel ou dont la réclamation auprès du responsable de traitement est restée sans suite, peut porter plainte devant la HAPDP.

Article 109 : Recours contre les décisions de la HAPDP

Les sanctions et les décisions de la HAPDP sont susceptibles de recours devant le Conseil d'Etat.

Article 110 : Recours juridictionnel

Sans préjudice de tout autre recours, y compris le droit de saisir la HAPDP, toute personne concernée a droit à un recours juridictionnel effectif si elle estime que les droits que lui confère la présente loi ont été violés du fait d'un traitement de ses données à caractère personnel.

En cas d'atteinte grave et immédiate aux droits des personnes, la personne dont les droits et libertés sont violés, peut demander par voie de référé, à la juridiction compétente, d'ordonner, le cas échéant et sous astreinte, toute mesure nécessaire à la sauvegarde de ces droits.

CHAPITRE XVI : DES DISPOSITIONS TRANSITOIRES ET FINALES

Article 111 : Disposition transitoires

Les traitements de données opérés pour le compte de l'État, d'un établissement public, d'une collectivité territoriale ou d'une personne morale de droit privé gérant un service public et déjà créés sont notifiés à la HAPDP sans préjudice des demandes d'avis ultérieures.

A compter de sa date d'entrée en vigueur tous les traitements de données à caractère personnel doivent répondre aux prescriptions de la présente loi sous peine de sanctions prévues par la présente loi.

Article 112 : Abrogation et Publication

La présente loi qui abroge toutes dispositions antérieures contraires notamment la loi n° 2017-28 du 03 mai 2017 relative à la protection des données à caractère personnel, modifiée par la loi n°2019-71 du 24 décembre 2019 est publiée au Journal Officiel de la République du Niger et exécutée comme loi de l'Etat.

Fait à Niamey, le 16 décembre 2022

Signé : Le Président de la République

MOHAMED BAZOUM

Le Premier Ministre

OUHOUMOUDOU MAHAMADOU

Pour ampliation :

Le Secrétaire Général

Adjoint du Gouvernement

LARWANA IBRAHIM