15 JUILLET 2023
SOIXANTE QUATRIEME ANNEE – N°218 Bis PRIX : 2.000 Francs Dépôt légal 777

JOURNAL OFFICIEL

DE LA REPUBLIQUE GABONAISE

POUR LES ABONNEMENTS ET LES ANNONCES :
"DIRECTION DES PUBLICATIONS OFFICIELLES" - LIBREVILLE - B. P. 563 - TEL. : 01 76 20 00.
Ceux-ci sont payables d'avance, par mandat ou virement au nom de M. le Directeur "des Publications Officielles" à Libreville
Compte courant CDC N° 11500000915, Centre de Libreville.

SOMMAIRE

ACTES DE LA REPUBLIQUE GABONAISE

PARLEMENT

PRESIDENCE DE LA REPUBLIQUE

MINISTERE DE L'INTERIEUR

ACTES DE LA REPUBLIQUE GABONAISE

_____

PARLEMENT

_____

Loi n°025/2023 du 12 juillet 2023 portant modification de la loi n°001/2011 du 25 septembre 2011 relative à la protection des données à caractère personnel

L'Assemblée Nationale et le Sénat ont délibéré et adopté ;
Le Président de la République, Chef de l'Etat, promulgue la loi dont la teneur suit :

Article 1er : La présente loi, prise en application des dispositions des articles 1er et 47 de la Constitution, est relative à la protection des données à caractère personnel.

Chapitre Ier : Des dispositions générales

Section 1 : De l'objet et du champ d'application

Article 2 : La présente loi fixe les règles relatives à la collecte, au traitement des données personnelles et de la vie privée. Elle a pour objet, de mettre en place un dispositif permettant de lutter contre les atteintes à la vie privée susceptible d'être engendrées par la collecte, le traitement, la transmission, le stockage et l'usage des données personnelles.

Article 3 : Toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données personnelles la concernant, dans les conditions fixées par la présente loi.

Article 4 : La présente loi s'applique à :

-toute collecte, tout traitement, toute transmission, tout stockage et toute utilisation des données personnelles par une personne physique, par des personnes morales de droit public ou de droit privé ;
-tout traitement automatisé ou non des données personnelles contenues ou appelées à figurer dans un fichier, à l'exception des traitements mentionnés à l'article 5 de la présente loi ;
-tout traitement mis en œuvre par un responsable tel que défini à l'article 6 de la présente loi sur le territoire gabonais ou en tout lieu où la loi gabonaise s'applique ;
-tout traitement mis en œuvre par un responsable, établi ou non sur le territoire gabonais, qui recourt à des moyens de traitement situés sur le territoire gabonais, à l'exclusion des moyens qui ne sont utilisés qu'à des fins de transit sur ce territoire. Dans les cas visés au point 3 ci-dessus, le responsable du traitement doit désigner un représentant établi sur le territoire gabonais, sans préjudice d'actions qui peuvent être introduites à son encontre ;
-tout traitement des données personnelles concernant la sécurité publique, la défense, la recherche et la poursuite d'infractions pénales ou la sûreté de l'Etat, même liées à un intérêt économique ou financier important de l'Etat, sous réserve des dérogations que définit la présente loi et des dispositions spécifiques en la matière fixées par d'autres lois.

Article 5 : La présente loi ne s'applique pas :

-aux traitements des données personnelles mis en œuvre par une personne physique dans le cadre exclusif de ses activités personnelles ou domestiques, à condition toutefois que les données personnelles 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 personnelles et à seule fin de permettre à d'autres destinataires du service le meilleur accès possible.

Section 2 : Des définitions

Article 6 : Au sens de la présente loi, on entend par :

-**Accountability** : obligation pour les entreprises de mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données personnelles ;

-**Ad exchange ou « plateforme d'échanges publicitaires »** : plate-forme mettant automatiquement en relation les ordres d'achats venant des demand-side platforms et les inventaires disponibles proposés par les supply-side platforms, concernant les enchères en temps réel ;

-**Analyse d'impact sur la protection des données** : étude qui doit être menée lorsqu'un traitement de données est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées ;

-**Annotation** : procédé par lequel les données sont décrites manuellement afin d'être caractérisées ;

-**Algorithme** : description d'une suite d'étapes permettant d'obtenir un résultat à partir d'éléments fournis en entrée ;

-**Apprentissage supervisé** : procédé d'apprentissage automatique dans lequel l'algorithme s'entraîne à une tâche déterminée en utilisant un jeu de données assorties chacune d'une annotation indiquant le résultat attendu ;

-**Apprentissage automatique** : champ d'étude de l'intelligence artificielle qui vise à donner aux machines

la capacité d'« apprendre » à partir de données, via des modèles mathématiques ;

-**Apprentissage non supervisé** : procédé d'apprentissage automatique dans lequel l'algorithme utilise un jeu de données brutes et obtient un résultat en se fondant sur la détection de similarités entre certaines de ces données ;

-**Augmentation de données** : processus d'augmentation de données qui accroît la quantité de données d'entraînement par la création de nouvelles données à partir des données existantes ;

-**Apprentissage par renforcement** : procédé d'apprentissage automatique consistant, pour un système autonome, à apprendre les actions à réaliser, à partir d'expériences, de façon à optimiser une récompense quantitative au cours du temps ;

-**Attaque par exemples contradictoires** : attaque visant à soumettre des entrées malicieuses ou corrompues au système d'intelligence artificielle en phase de production ou encore, c'est le fait de modifier une image de façon à tromper un classifieur d'image et ainsi attribuer une image dégradante à une personne ;

-**Attaque par force brute** : attaque consistant à tester, l'une après l'autre, chaque combinaison possible d'un mot de passe ou d'une clé pour un identifiant donné afin de se connecter à un service ciblé ;

-**Base légale d'un traitement** : autorise légalement sa mise en œuvre, ce qui donne le droit à un organisme de collecter ou d'utiliser des données personnelles. On peut également parler de « fondement juridique » ou de « base juridique » du traitement ;

-**Backdoor ou porte dérobée** : consiste à prévoir un accès tenu secret vis-à-vis de l'utilisateur légitime aux données contenues dans un logiciel ou sur un matériel ;

-**Biométrie** : analyse mathématique des caractéristiques biologiques d'une personne, destinée à déterminer son identité de manière irréfutable, notamment les empreintes digitales, l'iris, la rétine, la main, les empreintes vocales, l'acide désoxyribonucléique et tous autres signes distinctifs ;

-**Bourrage d'identifiant** : consiste à réaliser, à l'aide de logiciels ou de façon manuelle, des tentatives d'authentification massives sur des sites et services web à partir de couples identifiants ou mots de passe ;

-**Blockchain** : technologie de stockage et de transmission d'informations, transparente, sécurisée, et fonctionnant sans organe central de contrôle. Elle constitue une base de données qui contient l'historique de tous les échanges effectués entre ses utilisateurs ;

-**Bringyourowndevice** : pratique qui consiste à utiliser ses équipements personnels dans un contexte professionnel ;

-**Captation** : enregistrement d'une image par un dispositif, par exemple une caméra de vidéosurveillance ;

-**Termes simplifiés à privilégier** : film, enregistrement ;

-**Caractéristiques** : variable utilisée pour représenter une propriété définie d'une entité ou d'un objet. Il peut s'agir d'informations relatives à la forme, la texture, ou encore à la couleur ;

-**Catégories de données personnelles** : types d'informations recueillies sur l'identité, situation familiale, économique ou financière, données bancaires, données de connexion, donnés de localisation ;

-**Certification** : procédure par laquelle un organisme d'évaluation externe va donner l'assurance écrite qu'une personne, un produit, un processus ou un service est en conformité avec les exigences données dans un référentiel ;

-**CNAME CLOAKING ou « délégation de sous-domaine »** : délégation de la gestion d'un sous-domaine de l'éditeur à un tiers via une redirection. Cela permet à ce tiers de déposer, sur le terminal de l'utilisateur ;

-**Code de conduite** : ensemble des règles visant à instaurer un usage correct des ressources informatiques, de l'internet et des communications électroniques de la structure concernée et homologuée par l'Autorité nationale chargée de la protection des données personnelles et de la vie privée, notamment les chartes d'utilisation, élaborées par le responsable du traitement ;

-**Communications électroniques** : émissions, transmissions ou réceptions des signes, des signaux, d'écrits, d'images ou des sons par voie électronique ;

-**Communication par transmission** : mode de communication qui privilégie la transmission directe des données personnelles entre deux machines, un émetteur actif et un récepteur passif ;

-**Consentement de la personne concernée** : toute manifestation de volonté expresse, non équivoque, libre, spécifique et informée par laquelle la personne concernée ou son représentant légal, judiciaire ou conventionnel, accepte que ses données personnelles fassent l'objet d'un traitement manuel ou électronique ;

-**Copies temporaires** : données copiées temporairement dans un espace dédié, pour une durée limitée dans le temps, pour les besoins du fonctionnement du logiciel ;

-**Cookie** : petit fichier déposé à partir d'un serveur sur un disque dur d'un terminal à l'insu de l'internaute, lors de la consultation de certains sites Web, et qui conservent des informations en vue d'une connexion ultérieure ;

-**Cookie de capping** : traceur utilisé pour limiter le nombre de répétitions d'un contenu publicitaire à un même utilisateur ;

-**Cookie matching** : système qui permet de faire coïncider les identifiants publicitaires d'un même utilisateur entre différents réseaux publicitaires. Lorsque deux réseaux publicitaires tracent la même personne ;

-**Cookie zombie ou supercookie** : cookie qui utilise des méthodes tierces pour régénérer l'identifiant permettant de tracer l'utilisateur même quand celui-ci est supprimé ;

-**Co-responsable du traitement** : responsable du traitement qui détermine conjointement avec d'autres les finalités et les moyens du traitement de données personnelles ;

-**Classification** : méthode de catégorisation qui consiste à attribuer une classe ou catégorie à une entrée qui lui est soumise en fonction de sa proximité à la classe en question selon des critères bien choisis ;

-**Clauses contractuelles types** : modèles de clauses contractuelles permettant d'encadrer les transferts de données personnelles effectués par des responsables de traitement vers des destinataires situés dans les pays tiers ;

-**Cloud computing** : utilisation de la mémoire et des capacités de calcul des ordinateurs et des serveurs répartis dans le monde entier et liés par un réseau ;

-**Déclarant** : personne physique ou morale responsable d'un traitement ou d'un fichier contenant des données personnelles ;

-**Destinataire d'un traitement des données personnelles** : toute personne habilitée à recevoir 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 les données ;

-**Domaine d'emploi** : description de l'environnement et de la population visée par le procédé d'apprentissage automatique ;

-**Données personnelles** : toute information se rapportant à une personne physique identifiée ou identifiable directement ou indirectement par référence à un numéro d'identification en ligne ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturel ou social ;

-**Donnée biométrique** : caractéristique physique ou biologique permettant d'identifier une personne ;

-**Donnée brute dans le domaine de l'intelligence artificielle** : donnée n'ayant subi aucune transformation depuis son observation initiale ;

-**Donnée d'entrée dans le domaine de l'intelligence artificielle** : donnée utilisée pour l'apprentissage automatique ou la prise de décision du système d'intelligence artificielle ;

-**Données relatives à la santé** : toute information concernant l'état physique et mental d'une personne concernée, y compris les données génétiques, les prestations de services des soins de santé qui relèvent des informations sur l'état de santé passé, actuel et futur ;

-**Données sensibles** : toutes les données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques, les convictions religieuses ou l'appartenance syndicale des personnes, les données biométriques et génétiques, ainsi que les données relatives à la santé, à la vie sexuelle ou à l'orientation sexuelle de celles-ci ;

-**Donnée de sortie** : valeur représentant tout ou partie de l'opération effectuée par le système d'intelligence artificielle à partir des données d'entrée ;

-**Droit à la vie privée** : garantie pour toute personne physique de ne pas faire l'objet d'immixtion dans sa vie privée, celle de sa famille, dans son domicile, sa correspondance, ni de porter atteinte à son honneur et à sa réputation, en violation de ses droits et libertés, par tout support physique ou virtuel, autorisé ou non ;

-**Droit à l'information** : toute personne a un droit de regard sur ses propres données ; par conséquent, quiconque met en œuvre un fichier ou un traitement de données personnelles est obligé d'informer les personnes concernées ;

-**Droit d'accès** : droit pour toute personne de prendre connaissance de l'intégralité des données la concernant dans un fichier en s'adressant directement à ceux qui les détiennent, et en obtenir une copie dont le coût ne peut dépasser celui de la reproduction ;

-**Droit d'accès indirect ou d'exception** : droit pour toute personne de demander que l'Autorité pour la Protection des Données Personnelles et de la Vie Privée vérifie les renseignements qui peuvent la concerner dans les fichiers intéressant la sûreté de l'État, la défense et la sécurité publique ;

-**Droit de rectification** : droit pour toute personne de faire rectifier, compléter, actualiser, verrouiller ou effacer des informations la concernant lorsque des erreurs ont été décelées, des inexactitudes ou la présence de données dont la collecte ou l'utilisation ;

-**Droit d'opposition** : possibilité de s'opposer, pour des motifs légitimes, à figurer dans un fichier, et peut refuser sans avoir à se justifier, que les données qui la concernent soient utilisées à des fins de prospection commerciale ;

-**Droit au déréférencement** : droit de reconnaître les moteurs de recherche en tant que responsables de traitement ;

-**Drone** : appareil sans pilote à bord, généralement piloté à distance par un opérateur humain. C'est avant tout une plate-forme de capteurs mobiles, un engin d'observation, d'acquisition et de transmission de données géo-localisées ;

-**Echantillon** : fraction représentative d'une population ou d'un univers statistique ;

-**E-commerce/commerce électronique** : activité économique par laquelle une personne propose ou assure, à distance et par voie électronique, la fourniture des biens ou la prestation de services ;

-**Effacement** : technique qui permet à une personne concernée d'user du droit d'obtenir du responsable de traitement la suppression dans un délai raisonnable des données à caractère personnel la concernant ;

-**Ensemble d'entraînement ou d'apprentissage dans le domaine de l'intelligence artificielle** : jeu de données utilisé lors de la phase entraînement ou d'apprentissage : le système s'entraîne sur ces données pour effectuer la tâche attendue de lui ;

-**Ensemble de test dans le domaine de l'intelligence artificielle** : jeu de données utilisé lors de la phase de test ;

-**Ensemble de validation dans le domaine de l'Intelligence Artificielle** : jeu de données utilisé lors de la phase de validation ;

-**Entraînement dans le domaine de l'Intelligence Artificielle** : processus de l'apprentissage automatique pendant lequel le système d'Intelligence Artificielle construit un modèle à partir de données ;

-**Explicabilité** : capacité de mettre en relation et de rendre compréhensible les éléments pris en compte par le système d'Intelligence Artificielle pour la production d'un résultat ;

-**Ent espace numérique de travail** : tout ensemble intégré de services numériques choisis et mis à disposition de tous les acteurs de la communauté éducative d'un ou plusieurs établissements de l'enseignement scolaire ou de l'enseignement supérieur dans un cadre de confiance défini par un schéma ;

-**Fichier de données personnelles** : tout ensemble structuré de données accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique ;

-**Fichier automatisé** : tout ensemble d'informations faisant l'objet d'un traitement automatisé ;

-**Finalité du traitement** : objectif principal de l'utilisation de données personnelles. Les données sont collectées pour un but bien déterminé et légitime et ne sont pas traitées ultérieurement de façon incompatible avec cet objectif initial ;

-**Fonction d'activation dans le domaine de l'Intelligence Artificielle** : équivalent du « potentiel d'activation » qu'on retrouve dans les neurones biologiques. Cette fonction détermine si un neurone artificiel doit être activé ou pas ;

-**Formalités préalables** : ensemble des formalités déclaratives à effectuer auprès de l'Autorité pour la Protection des Données Personnelles et de la Vie Privée avant la mise en œuvre d'un traitement de données personnelles. Selon les cas, il peut s'agir d'une déclaration ou d'une demande d'autorisation ;

-**Flux transfrontalier** : données personnelles qui concernent les deux côtés d'une frontière ;

-**Géolocalisation** : technologie permettant de déterminer la localisation d'un objet ou d'une personne avec une certaine précision. Elle s'appuie généralement sur le système GPS ou sur les interfaces de communication d'un téléphone mobile ;

-**Impression** : affichage d'un contenu publicitaire à un utilisateur. Le nombre d'impressions est un indicateur notamment utilisé dans la publicité ;

-**Identité numérique** : ensemble des traces numériques qu'une personne ou une collectivité laisse sur internet. L'identité numérique ou IDN, peut être constituée par : un pseudo, un nom, des images, des vidéos, des adresses IP, des favoris, des commentaires ;

-**Identifiant sectorielle** : numéro d'identification attribué à une personne lors de son inscription au registre secteur d'activités de traitement tenu par le responsable du traitement et qui permet de l'identifier au sein du système d'information spécifique ;

-**Identifiant unique public** : numéro d'identification attribué à chaque personne lors de la première inscription de celle-ci au Registre National qui permet d'identifier chaque personne au sein du système d'information ;

-**Informatique** : science de traitement automatique et rationnel des informations en tant que support des connaissances et des communications ;

-**Injonction sous astreinte** : ordre de se mettre en conformité accompagné d'une somme à payer en cas de non-respect de la décision. La décision qui force le paiement de cette somme s'appelle une liquidation d'astreinte ;

-**Intelligence Artificielle** : procédé logique et automatisé reposant généralement sur un algorithme qui est en mesure de réaliser des tâches bien définies. Constitue une intelligence artificielle, tout outil utilisé par une machine ;

-**Interconnexion des données personnelles** : tout mécanisme de connexion consistant en la mise en relation des données traitées pour une finalité déterminée avec d'autres données traitées pour des finalités identiques ou non, ou liées par un ou plusieurs responsables de traitement ; elle peut être à sens unique, bidirectionnelle, ponctuelle, permanente ou aboutir à la création de nouveaux flux ;

-**Inventaire** : un espace publicitaire réservé qui est vendu par l'éditeur. Ces espaces ne sont généralement pas mis sur le marché directement par l'éditeur ;

-**Jeux numériques** : concept associé à l'émergence de l'ère numérique en tant que contexte culturel pour la croissance et le développement des jeunes enfants au 21ème siècle ;

-**Liberté** : faculté reconnue à chaque être humain d'agir, de penser, de s'exprimer selon ses propres choix, sans enfreindre les lois et règlements en vigueur ;

-**Limitation du traitement** : marquage de données personnelles conservées, en vue de limiter leur traitement futur ;

-**Liste d'opposition** : recensement des personnes qui ont fait connaître leur opposition à être prospectées dans le cadre d'opérations de marketing ;

-**Minimisation** : principe qui prévoit que les données personnelles doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées ;

-**Mise en demeure** : mesure prise par l'Autorité pour la Protection des Données Personnelles et de la Vie Privée qui énumère les manquements reprochés à l'organisme mis en cause ainsi que les mesures qu'il doit prendre, pour se mettre en conformité dans un délai fixé. À ce stade, la procédure de sanction n'est pas encore engagée ;

-**Modèle discriminatif** : modèle capable de réaliser une prédiction quant à l'appartenance à une classe pour des données nouvelles sur la base d'un apprentissage réalisé auparavant sur un jeu de données d'entraînement ;

-**Modèle génératif** : modèle défini par opposition à un modèle discriminatif. Il permet à la fois de générer de nouveaux exemples à partir des données d'entraînement et d'évaluer la probabilité qu'un nouvel exemple provienne ou ait été généré à partir des données d'entraînement ;

-**Objets connectés** : objets qui captent, stockent, traitent et transmettent des données, qui peuvent recevoir et donner des instructions et qui ont pour cela la capacité à se connecter à un réseau d'informations ;

-**Paramètre dans le domaine de l'Intelligence Artificielle** : propriété apprise des données utilisées pour l'entraînement ;

-**Partitionnement de données** : méthode ayant pour but de diviser un ensemble de données en différents sous-ensembles homogènes, c'est-à-dire partageant des caractéristiques communes ;

-**Personne concernée** : toute personne physique ou décédée qui fait l'objet d'un traitement des données personnelles ;

-**Personne physique identifiable** : toute personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel que le nom, le numéro d'identification, les données de localisation ou l'identifiant en ligne ;

-**Plateforme d'achat** : intermédiaires permettant aux régies publicitaires et annonceurs de réaliser leurs achats d'inventaires. Elles transfèrent ensuite ces ordres d'achat sur des plates-formes d'échanges publicitaires ;

-**Plateforme de gestion du consentement** : elle permet aux éditeurs de site web ou d'applications mobiles de mettre facilement en place une interface de recueil du consentement des utilisateurs. L'interface utilisée doit afficher une fenêtre contextuelle lors de la première visite ;

-**Plateforme de gestion des données** : service effectuant la collecte et la gestion de données utilisateurs, souvent provenant de sources en ligne, mais aussi hors-ligne ;

-**Plateforme numérique** : interface dématérialisée qui facilite l'accès à divers contenus, informations, services, biens etc… le tout délivré par des tiers ;

-**Portabilité** : technique qui offre à une personne concernée la possibilité de récupérer une partie de ses données dans un format ouvert et lisible par machine, lui permettant de les stocker ou les transmettre facilement d'un système d'information à un autre, en vue de leur réutilisation à des fins personnelles ;

-**Profilage** : traitement utilisant les données personnelles d'un individu en vue d'analyser et de prédire son comportement, déterminer ses performances au travail, sa situation financière, sa santé, ses préférences, ses habitudes de vie ;

-**Prospective 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 vendant des biens ou fournissant des services ;

-**Protection des mineurs à l'ère du numérique** : concerne l'exercice des droits des mineurs relatifs à ces données personnelles face à l'innovation numérique ;

-**Publicité ciblée ou personnalisée** : toute technique publicitaire qui vise à identifier les personnes individuellement afin de leur diffuser des messages publicitaires spécifiques en fonction de caractéristiques individuelles. Elle nécessite donc de connaître la personne ;

-**Publicité contextuelle** : toute technique publicitaire qui vise à diffuser sur un support web ou télévision des publicités choisies en fonction du contexte dans lequel le contenu publicitaire est inséré ;

-**Publicité programmatique** : toute diffusion de campagnes publicitaires, notamment ciblées, l'achat d'inventaires ne peut généralement pas se faire au cas par cas. La publicité programmatique permet donc de planifier l'achat automatique d'éléments d'inventaire selon des critères prédéfinis ;

-**Réduction de dimension ou dimensionnalité** : toute méthode permettant de diminuer la quantité d'informations en ne conservant que le strict nécessaire, permettant ainsi d'obtenir plus d'efficacité en termes de résultats et de temps d'analyse. Cette réduction de l'information utile peut se faire par sélection des données ;

-**Reconnaissance faciale** : technique qui permet à partir des traits de visage d'authentifier une personne, vérifier qu'une personne est bien celle qu'elle prétend être, de l'identifier au sein d'un groupe d'individus, dans un lieu, une image ou une base de données ;

-**Responsable du traitement** : toute personne physique, morale, publique ou privée, tout autre organisme ou association qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données personnelles, sauf désignation expresse par les textes en vigueur ;

-**Renouvellement** : procédé par lequel le détenteur des autorisations et récépissés de déclaration expirées, introduit de nouvelles demandes de traitements en tenant compte du délai de validité ;

-**Réseaux sociaux** : sites internet qui permettent aux utilisateurs, professionnels ou particuliers, de partager des informations ;

-**Robustesse dans le domaine de l'Intelligence Artificielle** : capacité du système à maintenir sa conformité à des exigences de performance ou de sécurité en présence de données d'entrée extérieures à son domaine d'emploi ;

-**Segmentation des données** : toute méthode permettant la division d'un corpus de données en plusieurs ensembles, soit à partir de critères objectifs soit de manière aléatoire ;

-**Service de la société de l'information** : toute activité économique accomplie à distance et par voie électronique portant sur des biens, des services, des droits ou des obligations ;

-**Signature électronique** : signature obtenue par un algorithme de chiffrement asymétrique permettant d'authentifier l'émetteur d'un message et d'en vérifier l'intégrité ;

-**Sous-traitant** : toute personne physique ou morale, publique ou privée, tout organisme ou association qui traite des données pour le compte du responsable du traitement et sous ses instructions ;

-**Système d'alerte professionnelle** : tout dispositif permettant aux membres d'une organisation et aux tiers d'alerter de manière confidentielle sur des actes contraires aux lois, au règlement intérieur de l'organisation ou de son code de conduite ;

-**Taux d'apprentissage** : tout facteur multiplicatif appliqué au gradient. À chaque itération, l'algorithme de descente de gradient multiplie le taux d'apprentissage par le gradient ;

-**Technologies de l'Information et de la Communication** : ensemble des techniques utilisées dans le traitement et la transmission des informations,

principalement de l'Informatique, de l'Internet et des Télécommunications ;

-**Télémédecine** : pratique médicale à distance utilisant les technologies de l'information et de la communication. Elle permet d'établir un diagnostic, d'assurer, pour un patient à risque, un suivi à visée préventive ou un suivi post-thérapeutique, de requérir un avis spécialisé, de préparer une décision thérapeutique, de prescrire des produits, de prescrire ou de réaliser des prestations ou des actes, ou d'effectuer une surveillance de l'état des patients ;

-**Test dans le domaine de l'Intelligence Artificielle** : processus consistant à évaluer les performances d'un système et à rechercher des erreurs liées à l'exécution d'un algorithme ou d'un programme en s'appuyant sur des jeux de données d'entrée ;

-**Tiers** : toute personne physique, morale, publique ou privée autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placée sous l'autorité directe du responsable du traitement ou du sous-traitant, est habilitée à traiter les données ;

-**Tiers autorisé** : toute autorité publique ou administration autorisée par une base légale à recevoir des informations personnelles ;

-**Traitement des données personnelles** : toute opération ou tout ensemble d'opérations effectuées à l'aide de procédés automatisés ou non et appliquées à des données ou à des ensembles de données personnelles ;

-**Traitement automatisé** : toutes opérations suivantes effectuées en totalité ou en partie à l'aide de procédés automatisés : enregistrement des données, application à ces données d'opérations logiques ou arithmétiques, leurs modifications, effacement, extraction ou diffusion ;

-**Traitement automatique de la parole** : toutes disciplines dont l'objectif est la captation, la transmission, l'identification et la synthèse de la parole. Ces disciplines rassemblent notamment la reconnaissance de la parole, la synthèse de la parole, l'identification du locuteur ;

-**Traitement automatique du langage naturel** : tout domaine multidisciplinaire impliquant la linguistique, l'informatique et l'intelligence artificielle. Il vise à créer des outils capables d'interpréter et de synthétiser le texte pour diverses applications ;

-**Traitement manuel** : tout traitement de données personnelles qui n'est pas nécessairement informatisé : les fichiers papier sont également concernés et doivent être protégés dans les mêmes conditions. Le traitement doit avoir un objectif, une finalité déterminée préalablement au recueil des données et à leur exploitation ; tels que la tenue du registre des sous-traitants, gestion des paies, gestion des ressources humaines ;

-**Transaction électronique** : action ou ensemble d'actions de nature commerciale ou non, portant notamment sur les biens ou les services en ligne ;

-**Transfert de données** : toute communication, copie ou déplacement de données personnelles ayant vocation à être traitées dans un pays tiers ;

-**Validation dans le domaine de l'Intelligence Artificielle** : tout processus consistant à expérimenter, observer et optimiser, en modifiant les hyperparamètres notamment, le comportement du système lors de son exécution ;

-**Vidéoprotection** : dispositif dit de « vidéoprotection » qui filme la voie publique et les lieux ouverts au public et sont soumis aux mesures de sécurité intérieure ;

-**Vidéosurveillance** : tout système de caméras et de transmission d'images permettant de surveiller ou d'enregistrer sur place ou à distance des lieux publics ou privés ;

-**Violation de données** : tout accès accidentel ou non autorisé à des données à caractère personnel, leur destruction, perte, utilisation, modification ou divulgation en violation du principe de la sécurité des données et ayant entraîné la copie, la transmission, la consultation, le vol de données personnelles ou leur utilisation par une personne physique ou morale non autorisée à le faire ;

-**Télévidéosurveillance** : tout système de vidéosurveillance qui permet d'alerter un centre d'appel en cas d'évènements inhabituels détectés sur des sites dont on souhaite assurer la protection ;

-**Vie privée** : vie cachée qui se rapporte à l'intimité d'une personne dans sa relation avec autrui au sujet de sa vie sentimentale, familiale, sa santé, sa résidence, sa correspondance, son domicile et son image ;

-**Violation de données personnelles** : non-respect des formalités préalables à la mise en œuvre des traitements des données à caractère personnel ou la violation de la sécurité, entraînant de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données personnelles transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données ;

-**Vision par ordinateur** : branche de l'intelligence artificielle dont le principal but est de permettre à une

machine d'analyser et traiter une ou plusieurs images ou vidéos prises par un système d'acquisition.

Chapitre II : De l'autorité pour la protection des données personnelles et de la vie privée

Section 1 : De la création et des missions

Article 7 : Il est créé, une Autorité chargée de veiller à la Protection des Données Personnelles et de la Vie Privée en République Gabonaise, dénommée Autorité pour la Protection des Données Personnelles et de la Vie Privée, en abrégé APDPVP.

L'APDPVP est une autorité administrative indépendante.

Article 8 : L'APDPVP a pour missions d'informer toute personne concernée et tout responsable de traitements de leurs droits et obligations, ainsi que de veiller à la mise en œuvre du traitement des données personnelles et des atteintes à la vie privée.

En outre, l'APDPVP assure la veille technologique de l'information en collaboration avec les autres administrations concernées et rend publique, le cas échéant, son appréciation des conséquences qui en résultent pour l'exercice des droits et libertés.

À ce titre, elle est notamment chargée :

-d'autoriser les traitements mentionnés à l'article 80 et donne un avis sur les traitements mentionnés aux articles 81 et 82 et reçoit des déclarations relatives aux autres traitements ;
-d'établir et publier les normes mentionnées à l'alinéa 1er de l'article 79 et édicte, le cas échéant, des règlements types en vue d'assurer la sécurité des systèmes ;
-de recevoir des réclamations, pétitions et plaintes relatives à la mise en œuvre des traitements des données personnelles et informer leurs auteurs des suites données à celles-ci ;
-de répondre aux demandes d'avis des pouvoirs publics et, le cas échéant, des juridictions, et conseiller les personnes et organismes qui mettent en œuvre ou envisagent de mettre en œuvre des traitements automatisés des données personnelles ;
-d'informer, sans délai, le Procureur de la République des infractions dont elle a connaissance et présenter, le cas échéant, les observations en rapport avec la loi pénale ;
-de prendre, par décision particulière, de charger un ou plusieurs de ses membres ou ses agents à procéder à des vérifications portant sur tout traitement de données personnelles et, le cas échéant, à obtenir des copies de tout document ou support d'informations utile à ses missions, dans les conditions prévues aux articles 197 et 198 ;
-de prononcer à l'égard d'un responsable de traitement, l'une des mesures et sanctions prévues par les articles 199 à 204 ;
-de répondre aux demandes d'accès des traitements des données personnelles des personnes concernées ;
-de donner un avis sur la conformité aux dispositions de la présente loi des projets de règles professionnelles ainsi que des produits et procédures tendant à la protection des personnes à l'égard du traitement des données personnelles, ou à l'anonymisation de ces données, qui lui sont soumises ;
-de porter une appréciation sur les garanties offertes par des règles professionnelles qu'elle a précédemment reconnues conformes aux dispositions de la présente loi, au regard du respect des droits fondamentaux des personnes ;
-de délivrer un label à des produits ou à des procédures tendant à la protection des personnes à l'égard du traitement des données personnelles, après qu'elle les a reconnus conformes aux dispositions de la présente loi ;
-de donner des avis sur tout projet de loi ou décret relatif à la protection des personnes à l'égard des traitements automatisés ;
-de proposer au Gouvernement des mesures législatives ou réglementaires d'adaptation de la protection des libertés à l'évolution des procédés et techniques informatiques ;
-d'apporter, à la demande d'autres organismes et administrations, son concours en matière de protection des données personnelles ;
-de s'associer, à la demande du Gouvernement, à la préparation et à la définition de la position gabonaise dans les négociations internationales dans le domaine de la protection des données personnelles et de la vie privée ;
-de faire partie, à la demande du Gouvernement, de la délégation gabonaise aux travaux des organisations communautaires et internationales compétentes dans le domaine de la protection des données personnelles et de la vie privée.

Article 9 : Pour l'accomplissement de ses missions, l'APDPVP peut procéder par voie de recommandation et prendre des décisions individuelles ou réglementaires dans les cas prévus par la présente loi.

Article 10 : L'APDPVP présente chaque année au Président de la République, au Gouvernement et au Parlement un rapport public rendant compte de l'exécution de sa mission.

Section 2 : De la composition

Article 11 : L'APDPVP est composée de commissaires permanents et de commissaires non permanents.

Les membres de l'APDPVP sont choisis en raison de leurs compétences avérées dans le domaine du numérique et des questions touchant aux libertés individuelles.

Ils sont nommés par décret pris en Conseil des Ministres.

Article 12 : Les commissaires permanents sont au nombre de neuf.

Ils sont désignés comme suit :

-trois personnalités désignées par le Président de la République, dont le président de l'APDPVP ;
-un magistrat du Conseil d'Etat désigné sur proposition du président du Conseil d'Etat ;
-un magistrat de la Cour de Cassation désigné sur proposition du président de la Cour de Cassation ;
-un avocat désigné par l'Ordre des Avocats ;
-un médecin désigné par l'Ordre des Médecins ;
-un représentant des organisations de défense des Droits de l'Homme désigné par ses pairs ;
-un expert en économie numérique désigné par le Ministre chargé de l'Economie Numérique.

Article 13 : Les commissaires non permanents sont au nombre de quatre.

Ils sont désignés comme suit :

-un député désigné par le président de l'Assemblée Nationale ;
-un sénateur désigné par le président du Sénat ;
-un commissaire du Gouvernement désigné par le Premier Ministre ;
-un représentant du patronat gabonais désigné par ses pairs.

Article 14 : Les commissaires non permanents prennent part aux sessions de la l'APDPVP. Ils ont voix consultative.

Le commissaire du Gouvernement présente lors des sessions de l'Autorité toute observation ou orientation du Gouvernement sur un projet de délibération.

Article 15 : Les commissaires perçoivent une rémunération et des avantages qui leur assurent une indépendance matérielle et morale dans l'exercice de leurs fonctions.

Cette rémunération et ces avantages sont fixés par voie réglementaire.

Section 3 : Des organes

Article 16 : Les organes de l'APDPVP sont :

-le bureau ;
-la formation plénière ;
-la formation restreinte.

Article 17 : Le bureau de l'APDPVP est composé de cinq membres :

-le président ;
-le vice-président ;
-le questeur ;
-le rapporteur ;
-le rapporteur adjoint.

Outre le président, les autres membres du bureau sont élus par leurs pairs.

La composition des cabinets du président et des autres commissaires Permanents de l'Autorité est fixée par décret.

En cas d'empêchement temporaire ou définitif d'exercice de ses fonctions pour raison quelconque, le vice-président assure les fonctions de président de l'APDPVP dans le cadre du mandat.

Article 18 : Le bureau est l'organe directeur de l'APDPVP.

Article 19 : La formation plénière est l'organe de décision de l'APDPVP. En cas d'égalité des voix, celle du Président est prépondérante.

Article 20 : La formation restreinte est un organe de proposition au sein de l'APDPVP. Elle peut être chargée, par la formation plénière, d'exercer certaines attributions relatives à ses pouvoirs d'investigation.

Article 21 : L'APDPVP est représentée sur l'ensemble du territoire par des représentations provinciales, qui sont chargées de conduire les missions dévolues à l'Autorité.

Le représentant provincial est nommé par décret pris en Conseil de Ministre sur proposition du Président de l'Autorité de Protection parmi les agents publics permanents de la première catégorie. Les traitements et avantages sont arrêtés conformément aux textes en vigueur.

Section 4 : Du mandat, des incompatibilités et du statut disciplinaire

Article 22 : Le mandat des commissaires permanents est de cinq ans, renouvelable une fois.

Le renouvellement de l'ensemble des membres permanents, soit neuf, se fait au minimum au tiers de ses membres.

Les commissaires non permanents ayant un mandat électif siègent à la l'APDPVP pour la durée de ce mandat.

Le commissaire non-permanent désigné par le patronat siège à la l'APDPVP pour la durée fixée par cet organisme.

Article 23 : Le membre de l'APDPVP qui cesse d'exercer ses fonctions en cours de mandat est remplacé, dans les mêmes conditions, pour la durée du mandat restant à courir.

La qualité de commissaire permanent se perd en cours de mandat par :

-le décès ;
-la démission ;
-l'empêchement définitif constaté par l'APDPVP dans des conditions définies par son règlement intérieur.

L'APDPVP peut mettre fin, au terme d'une procédure contradictoire, aux fonctions d'un commissaire en cas de :

-méconnaissance par l'intéressé de ses obligations ;
-violation du régime des incompatibilités ;
-indélicatesse avérée ;
-participation irrégulière aux activités de l'Autorité ;
-manquements graves à la discipline de l'Autorité.

En cas de démission, décès ou incapacité définitive dûment constatée d'un commissaire, il est procédé, à la diligence du président de l'Autorité, à son remplacement, sauf si la fraction du mandat restant à courir est inférieure à six mois.

Le commissaire ainsi désigné achève le mandat commencé.

En cas de manquement à leurs obligations professionnelles ou à la discipline de l'Autorité, le questeur et le rapporteur sont démis de leurs fonctions sur proposition du président de l'Autorité et remplacés conformément au vote du collège des membres.

Article 24 : Avant leur entrée en fonction, les commissaires permanents prêtent devant la Cour de Cassation siégeant en audience solennelle, le serment dont la teneur suit : « je jure solennellement de bien et fidèlement remplir ma fonction de membre de l'Autorité pour la Protection des Données Personnelles et de la Vie Privée, en toute indépendance et impartialité de façon digne et loyale et de garder le secret des délibérations ».

Les agents de l'APDPVP cités à l'article 25 ci-dessous, prêtent serment devant le Tribunal de Première Instance de Libreville en ces termes : « je jure de bien et loyalement remplir mes fonctions d'agent de l'Autorité pour la Protection des Données Personnelles et de la Vie Privée en toute indépendance et impartialité et de garder le secret des délibérations ».

Article 25 : Les agents assermentés appelés à participer à la mise en œuvre des missions de contrôle doivent y être habilités par l'APDPVP.

Article 26 : Les commissaires et les agents sont astreints au secret professionnel pour les faits, actes ou renseignements dont ils ont pu avoir connaissance en raison de leurs fonctions.

Article 27 : Dans l'exercice de leurs attributions, les commissaires ne reçoivent d'instruction d'aucune autorité.

Les autorités publiques, les dirigeants d'entreprises publiques ou privées, les responsables de groupements divers et, plus généralement, les détenteurs ou utilisateurs de traitements ou de fichiers des données personnelles, ne peuvent s'opposer à l'action de l'APDPVP. Ils doivent prendre toutes les mesures utiles afin de faciliter sa tâche.

Sauf dans les cas où elles sont astreintes au secret professionnel, les personnes interrogées dans le cadre des vérifications faites par l'APDPVP sont tenues de fournir les renseignements demandés par celle-ci pour l'exercice de ses missions.

Article 28 : Les commissaires jouissent d'une immunité totale pour les opinions émises dans l'exercice ou à l'occasion de l'exercice de leurs fonctions.

Article 29 : La qualité de commissaire est incompatible avec celle de membre du Gouvernement.

Article 30 : Aucun commissaire ne peut :

-participer à une délibération ou procéder à des vérifications relatives à un organisme au sein duquel il détient un intérêt, direct ou indirect, exerce des fonctions ou détient un mandat ;
-participer à une délibération ou procéder à des vérifications relatives à un organisme au sein duquel il a, au cours des trente-six mois précédant la délibération ou les vérifications, détenu un intérêt direct ou indirect, exercé des fonctions ou détenu un mandat.

Article 31 : Tout commissaire est tenu d'informer le président :

-des intérêts directs ou indirects qu'il détient ou pourrait détenir ;
-des fonctions qu'il exerce ou vient à exercer ;
-de tout mandat qu'il détient ou pourrait détenir au sein d'une personne morale.

Le Président est astreint aux mêmes obligations d'information.

Ces informations sont tenues à la disposition de l'APDPVP.

Article 32 : Tout manquement aux obligations mentionnées à l'article 30 ci-dessus entache de nullité les délibérations concernées et peut donner lieu à suspension du commissaire concerné.

Section 5 : Du fonctionnement

Article 33 : Un Secrétariat Général assure l'administration de l'Autorité pour la Protection des Données Personnelles et de la Vie Privée.

Le Secrétariat Général est dirigé par un Secrétaire Général nommé par décret pris en Conseil des Ministres, sur proposition du président de l'APDPVP, parmi les administrateurs civils ou administrateurs économiques et financiers de la première catégorie, justifiant d'une expérience de dix ans au moins.

Il est assisté d'un Secrétaire Général Adjoint nommé dans les mêmes formes et conditions.

L'organisation du Secrétariat Général est fixée par voie réglementaire.

Article 34 : Les autres attributions, l'organisation et le fonctionnement du Secrétariat Général sont fixés par voie réglementaire.

Article 35 : Les règles relatives à l'organisation et au fonctionnement de l'APDPVP sont fixées par le règlement intérieur.

Section 6 : Des ressources

Sous-section 1 : Des ressources humaines

Article 36 : Les personnels de l'APDPVP sont constitués d'agents publics et de ceux régis par le Code du Travail.

Sous-section 2 : Des ressources financières

Article 37 : Les ressources de l'APDPVP sont constituées :

-de la dotation de l'Etat ;
-des contributions des partenaires au développement ;
-des recettes affectées ;
-des ressources propres.

Les ressources propres sont constituées :

-des frais applicables à certains services et actes rendus aux opérateurs économiques ;
-des pénalités résultant de son activité.

Article 38 : Les ressources propres citées à l'article ci-dessus sont versés à l'agence comptable.

Article 39 : L'APDPVP ne peut recevoir de don ou subvention d'un individu, d'un organisme ou d'un Etat étranger que par l'intermédiaire d'une structure de coopération de l'Etat Gabonais.

Article 40 : Le budget de l'APDPVP est préparé par le bureau et adopté par la formation plénière.

Article 41 : Les comptes de l'APDPVP sont présentés au contrôle de la Cour des Comptes.

Article 42 : Le Président de l'APDPVP est l'ordonnateur des recettes et des dépenses.

L'APDPVP dispose d'une agence comptable de rattachement.

Chapitre III : Des droits et obligations des personnes concernées par le traitement des données personnelles et de la vie privée

Section 1 : Des droits des personnes concernées

Sous-section 1 : Du droit d'accès

Article 43 : Toute personne physique justifiant de son identité a le droit de demander gratuitement, par écrit, quel que soit le support, au responsable d'un traitement des données personnelles, de lui fournir :

-la finalité du traitement ;
-la catégorie de données personnelles concernées ;
-les destinataires ou catégories de destinataires auxquels les données personnelles ont été ou sont communiquées ;
-les informations permettant de connaître et de contester le traitement ;
-la confirmation que des données personnelles la concernant font ou ne font pas l'objet de ce traitement ;
-la durée de conservation des données personnelles envisagée et les critères utilisés pour déterminer cette durée, lorsque cela est possible ;
-l'existence des droits qu'elle détient en vertu des dispositions de la présente loi ;
-le droit d'introduire une réclamation auprès de l'Autorité Nationale chargée de la Protection des Données Personnelles ;
-les transferts éventuels des données personnelles envisagés à destination d'un pays tiers ;
-la communication, sous une forme accessible et intelligible, des données personnelles qui la concernent ainsi que de toute information disponible quant à l'origine de celles-ci ;
-lorsque les données personnelles ne sont pas collectées auprès de la personne concernée, toute information disponible quant à leur source ;

-l'existence d'une prise de décision automatisée, y compris un profilage et, au moins en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée ;
-la personne concernée a le droit d'obtenir à sa demande connaissance du raisonnement qui sous-tend le traitement des données lorsque les résultats de ce traitement lui sont appliqués.

Lorsque les données personnelles sont transférées vers un pays tiers ou à une organisation internationale, la personne concernée a le droit d'être informée des garanties concernant ce transfert.

Le responsable du traitement fournit une copie des données personnelles faisant l'objet d'un traitement. Il peut exiger le paiement de frais raisonnables basés sur les coûts administratifs pour toute copie supplémentaire demandée par la personne concernée. Lorsque la personne concernée présente sa demande par voie électronique, les informations sont fournies sous une forme électronique d'usage courant, à moins que la personne concernée ne demande qu'il en soit autrement.

Le droit d'obtenir une copie ne porte pas atteinte aux droits et libertés d'autrui.

Article 44 : Une copie des données personnelles concernant l'intéressé est délivrée 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 personnelles, la personne concernée peut en informer l'Autorité nationale chargée de la Protection des Données Personnelles ou le juge compétent qui prend toute mesure de nature à éviter cette dissimulation ou cette disparition.

Article 45 : Toute personne qui, dans l'exercice de son droit d'accès, a des raisons sérieuses de croire que les données qui lui ont été communiquées ne sont pas conformes aux données traitées, peut en informer l'Autorité nationale chargée de la Protection des Données Personnelles qui procède aux vérifications nécessaires.

Article 46 : Le droit d'accès d'un patient à ses données de santé est exercé par lui-même ou par l'intermédiaire d'un médecin de son choix. En cas de décès du patient, le conjoint survivant, ses enfants, le cas échéant ses ayants-droit et, s'il s'agit d'un mineur, ses père et mère peuvent exercer, par l'intermédiaire d'un médecin qu'ils désignent, ce droit d'accès.

Article 47 : 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 auprès duquel elles sont adressées.

Article 48 : Par dérogation aux dispositions des articles 42 à 46 de la présente loi, lorsqu'un traitement intéresse la sûreté de l'Etat, la défense ou la sécurité publique, le droit d'accès s'exerce dans les conditions suivantes :

-la demande est adressée à l'Autorité pour la Protection des Données Personnelles et de la Vie Privée qui désigne l'un de ses membres appartenant ou ayant appartenu au Conseil d'Etat ou à la Cour de Cassation pour mener les investigations nécessaires. Celui-ci peut se faire assister d'un autre agent de l'Autorité nationale. Il est notifié au requérant qu'il a été procédé aux vérifications ;
-l'Autorité chargée de la Protection des Données Personnelles constate, en accord avec le responsable du traitement, que la communication des données qui y sont contenues ne met pas en cause ses finalités, la sûreté de l'Etat, la défense ou la sécurité publique, ces données peuvent être communiquées au requérant ;
-le traitement est susceptible de comprendre des informations dont la communication ne mettrait pas en cause les fins 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 49 : Les dispositions de l'article 47 ci-dessus s'appliquent au traitement mis en œuvre par les administrations et les personnes privées chargées d'une mission de service public en matière de prévention, de recherche ou de constatation des infractions, de contrôle ou recouvrement des impositions.

Sous-section 2 : Du droit de rectification et du droit à l'effacement

Article 50 : Toute personne peut demander directement que les informations détenues sur elle soient :

-rectifiées si elles sont inexactes ;
-complétées ou clarifiées si elles sont incomplètes ou équivoques ;
-mises à jour si elles sont obsolètes ;
-effacées si elles n'ont pas été régulièrement collectées et conservées ou si la finalité est détournée.

Article 51 : La personne concernée a le droit d'obtenir du responsable du traitement, dans les meilleurs délais, la rectification des données personnelles la concernant qui sont inexactes.

Article 52 : La personne concernée a le droit d'obtenir que les données personnelles incomplètes ou obsolètes soient complétées notamment par une déclaration

complémentaire ou mises à jour, compte tenu des finalités du traitement.

Article 53 : Toute personne justifiant de son identité a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, des données personnelles la concernant, notamment dans l'un des cas suivants :

-les données personnelles ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière ;
-la personne concernée retire le consentement sur lequel est fondé le traitement et qu'il n'existe pas d'autre fondement juridique au traitement ;
-les données personnelles ont fait l'objet d'un traitement illicite ;
-les données personnelles doivent être effacées pour respecter une obligation légale ;
-les données personnelles ont été collectées dans le cadre des services offerts par la société de l'information.

Lorsque les données personnelles ont été rendues publiques et que le responsable du traitement est tenu de les effacer en vertu de l'alinéa précédent, il prend des mesures raisonnables, y compris d'ordre technique, pour informer les tiers à l'égard desquels, la personne concernée a demandé l'effacement de tout lien vers ses données personnelles, ou toute copie ou reproduction de celles-ci.

Article 54 : Les dispositions de l'article 52 ci-dessus ne s'appliquent pas dans la mesure où le traitement est notamment nécessaire :

-à l'exercice du droit à la liberté d'expression et d'information ;
-au respect d'une obligation légale ou pour l'exercice d'une mission d'intérêt public dont est investi le responsable de traitement ;
-aux motifs d'intérêt public dans le domaine de la santé publique ;
-à des fins archivistiques dans l'intérêt public, de recherches scientifiques, historiques ou statistiques ;
-à une action en justice.

Sous-section 3 : Du droit à la limitation du traitement

Article 55 : La personne concernée a le droit d'obtenir du responsable du traitement, la limitation du traitement de ses données personnelles lorsque l'un des éléments suivants s'applique :

-l'exactitude des données personnelles est contestée par la personne concernée ;
-le traitement est illicite et la personne concernée s'oppose à l'effacement de ses données personnelles et exige en contrepartie, la limitation de leur utilisation ;
-le responsable du traitement n'a plus besoin des données personnelles aux fins du traitement, mais celles-ci sont encore nécessaires à la personne concernée pour la constatation, l'exercice ou la défense de droits en justice ;
-la personne concernée s'est opposée au traitement des données personnelles la concernant dans l'attente de la vérification du motif légitime du responsable du traitement.

Article 56 : Les données personnelles d'un traitement qui a été limité ne peuvent, à l'exception de la conservation, être traitées qu'avec le consentement de la personne concernée, ou pour la constatation, l'exercice ou la défense de droits en justice, ou pour la protection des droits d'une autre personne physique ou morale, ou encore pour des motifs importants d'intérêt public.

Article 57 : La personne concernée qui a obtenu la limitation du traitement de ses données en vertu des dispositions de l'article 54 ci-dessus, est informée par le responsable du traitement, avant que la limitation du traitement ne soit levée.

Sous-section 4 : Du droit à la portabilité des données personnelles

Article 58 : La personne concernée a le droit de recevoir les données la concernant qu'elle a fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine.

Elle a le droit de transmettre ces données personnelles à un autre responsable du traitement sans que le responsable du traitement auquel les données personnelles ont été communiquées y fasse obstacle, lorsque :

-le traitement est fondé sur le consentement ou sur un contrat ;
-le traitement est effectué à l'aide de procédés automatisés.

Article 59 : Lorsque la personne concernée exerce son droit à la portabilité des données personnelles en application de l'article 57 ci-dessus, elle a le droit d'obtenir que les données personnelles soient transmises directement d'un responsable du traitement à un autre, lorsque cela est techniquement possible.

Sous-section 5 : Du droit d'opposition

Article 60 : La personne concernée a le droit de s'opposer à tout moment, pour des raisons tenant à sa situation particulière, au traitement des données personnelles la concernant ayant pour fondement :

-l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité public dont est investi le responsable du traitement ;
-le traitement est nécessaire à l'exécution des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, y compris un profilage fondé sur ces dispositions.

Le responsable du traitement ne traite plus les données personnelles, à moins qu'il ne démontre qu'il existe des motifs légitimes et impérieux pour les traitements qui prévalent sur les intérêts, les droits et libertés de la personne concernée, ou pour la constatation, l'exercice ou la défense de droits en justice.

Article 61 : La personne concernée a le droit de s'opposer par tout moyen, gratuitement, à la communication ou à l'utilisation sur tout support de ses données personnelles, à des fins diverses si elle n'a pas préalablement consenti.

Le droit d'opposition ne s'applique pas lorsque le traitement est d'ordre public ou répond à une obligation légale ou contractuelle.

Article 62 : La personne concernée a le droit de s'opposer à tout moment au traitement des données personnelles la concernant, y compris au profilage dans la mesure où il est lié à une telle prospection, lorsque les données personnelles sont traitées à des fins de prospection.

Lorsque la personne concernée s'oppose au traitement à des fins de prospection, les données personnelles ne sont plus traitées à ces fins.

Article 63 : Le droit prévu par l'article 61 ci-dessus est explicitement porté à l'attention de la personne concernée et présenté clairement et séparément de toute autre information au plus tard, au moment de la première communication avec la personne concernée.

Article 64 : La personne concernée peut, dans le cadre de l'utilisation de services de la société de l'information, exercer son droit d'opposition à l'aide de procédés automatisés utilisant des spécifications techniques.

Article 65 : La personne concernée a le droit de s'opposer, pour des raisons tenant à sa situation particulière, au traitement de données personnelles la concernant, à moins que ce traitement ne soit nécessaire à l'exécution d'une mission d'intérêt public, lorsque des données personnelles sont traitées à des fins de recherche scientifique, historique ou statistiques.

Sous-section 6 : De la décision individuelle automatisée et du profilage

Article 66 : La personne concernée a le droit de s'opposer à une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative ou de façon similaire.

Article 67 : Les dispositions de l'article 65 ci-dessus ne s'appliquent que lorsque la décision est :

-nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et un responsable de traitement ;
-fondée sur le consentement explicite de la personne concernée.

Article 68 : Dans les cas prévus par l'article 66 ci-dessus, le responsable du traitement met en œuvre des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée, dont au moins, le droit d'obtenir une intervention humaine de la part du responsable du traitement, d'exprimer son point de vue et de contester la décision.

Article 69 : Les décisions prévues par l'article 66 de la présente loi ne peuvent être fondées sur des catégories particulières des données à caractère personnel, prévues par les articles 74 et 65, à moins que les articles 74 et 66 ne s'appliquent et que des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée ne soient mis en place.

Section 2 : Des conditions et obligations de mise en œuvre des données personnelles par les responsables de traitement

Sous-section 1 : Des conditions de licéité du traitement des données personnelles

Article 70 : Le traitement porte sur des données qui remplissent les conditions suivantes :

-les données sont collectées et traitées de manière loyale et licite ;
-elles sont collectées pour des finalités déterminées, explicites, légitimes et non inhumaines et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités ;
-elles sont adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs ;
-elles sont exactes, complètes et, si nécessaire, mises à jour ;
-les mesures appropriées doivent être prises pour que les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées soient effacées ou rectifiées ;
-elles sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées.

Toutefois, un traitement ultérieur des données à des fins statistiques, de recherche scientifique ou historique est considéré comme compatible avec les finalités initiales de la collecte des données, s'il est réalisé dans le respect des principes et des procédures prévues au présent chapitre ainsi qu'à la section I du chapitre V et s'il n'est pas utilisé pour prendre des décisions à l'égard des personnes concernées.

Article 71 : Un traitement des données doit avoir reçu le consentement de la personne concernée ou satisfaire à l'une des conditions suivantes :

-le respect d'une obligation légale incombant au responsable du traitement ;
-la sauvegarde de la vie privée de la personne concernée ;
-l'exécution d'une mission de service public dont est investi le responsable ou le destinataire du traitement ;
-l'exécution, soit d'un contrat auquel la personne concernée est partie, soit des mesures précontractuelles prises à la demande de celle-ci ;
-la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le destinataire, sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée.

Article 72 : Le responsable d'un traitement reposant sur le consentement de la personne concernée, doit être en mesure de démontrer que celle-ci a consenti au traitement de ses données.

Lorsque le consentement est donné dans le cadre d'une déclaration écrite qui concerne également d'autres questions, la demande de consentement est présentée sous une forme accessible, compréhensible et en des termes clairs et simples.

En matière de transaction électronique le consentement ne se présume pas et doit prendre la forme d'un acte de volonté univoque, par exemple au moyen d'une case à cocher.

L'acceptation des conditions générales d'utilisation ou de vente n'est pas considérée comme une modalité suffisante du recueil du consentement des personnes. Il est également recommandé au e-commerçant d'intégrer directement sur son site marchand un moyen simple de retirer, sans frais, le consentement ainsi donné.

Article 73 : La personne concernée a le droit de retirer son consentement à tout moment. Ce retrait ne compromet pas la licéité du traitement fondé sur le consentement donné avant celui-ci. La personne concernée est informée de ce droit avant de donner son consentement.

Article 74 : Le traitement des données relatives à un enfant est licite lorsque l'enfant est âgé d'au moins dix-huit ans.

Lorsque l'enfant est âgé de moins de dix-huit ans, le traitement des données est expressément autorisé par le titulaire de l'autorité parentale à l'égard de l'enfant.

Dans ce cas, le responsable du traitement s'assure, par tout moyen, que le consentement est donné par le titulaire de l'autorité parentale.

Article 75 : Il est interdit de collecter ou de traiter des données qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques, religieuses ou l'appartenance syndicale des personnes, les données biométriques et génétiques, ainsi que les données relatives à la santé et à la vie sexuelle.

Article 76 : Dans la mesure où la finalité du traitement l'exige, certaines catégories des données ne sont pas soumises à l'interdiction prévue par l'article 74 ci-dessus, notamment :

-le traitement pour lequel la personne concernée a donné son consentement express, sauf dans le cas où la loi prévoit que l'interdiction prévue par l'article 74 ci-dessus ne peut être levée par le consentement de la personne concernée ;
-le traitement nécessaire à la sauvegarde de la vie humaine auquel la personne concernée ne peut consentir par suite d'une incapacité juridique ou d'une impossibilité matérielle ;
-le traitement mis en œuvre par une association ou tout autre organisation à but non lucratif, à caractère religieux, philosophique, politique ou syndical pour les données sensibles correspondant à leur objet, sous réserve qu'ils ne concernent que leurs membres et, le cas échéant, les personnes qui entretiennent avec eux des contacts réguliers dans le cadre de leur activité, et qu'ils ne portent que sur des données non communiquées à des tiers, à moins que les personnes concernées n'y consentent expressément ;
-le traitement des données rendues publiques par la personne concernée ;
-le traitement des données nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice ;
-le traitement des données nécessaire aux fins de la médecine préventive, des diagnostics médicaux, de l'administration des soins, ou de la gestion de services de santé et mis en œuvre par un membre d'une profession de santé, ou par une autre personne à laquelle s'impose en raison de ses fonctions l'obligation de secret professionnel ;
-le traitement statistique réalisé à des fins économiques par les services statistiques des ministères compétents, dans le respect de la loi sur l'obligation, la coordination et le secret en matière de statistiques, après avis de l'administration compétente et dans les conditions prévues par l'article 78 de la présente loi ;

-le traitement nécessaire à la recherche dans le domaine de la santé selon les modalités prévues par la présente loi.

Lorsque les données sensibles sont appelées à faire l'objet à bref délai, d'un procédé d'anonymisation préalablement reconnu conforme aux dispositions de la présente loi par l'Autorité, celle-ci peut autoriser, compte tenu de leur finalité, certaines catégories de traitements selon les modalités prévues par la présente loi.

De même, ne sont pas soumis à l'interdiction prévue par l'article 77 les traitements, informatisés ou non, justifiés par l'intérêt public et autorisés dans les conditions prévues par les articles 82 et 83 de la présente loi.

Le traitement des données sensibles, notamment, les données génétiques, les données personnelles concernant les infractions, les procédures, les condamnations pénales et les mesures de sûretés connexes, les données biométriques identifiant un individu de façon unique, les données personnelles pour les informations qu'elles relèvent sur l'origine raciale ou ethnique, les opinions politiques, l'appartenance syndicale, les convictions religieuses, la santé ou la vie sexuelle, n'est autorisé que si la personne concernée a donné son consentement exprès, ce consentement doit être écrit et la personne doit avoir été informée au préalable de sorte que ce traitement ne présente aucun risque de discrimination.

Article 77 : Le traitement des données relatives aux infractions, condamnations et mesures de sûreté ne peut être mis en œuvre que par :

-les autorités publiques, judiciaires et les personnes morales gérant un service public, 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 par la loi.

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

Aucune autre décision produisant des effets juridiques à l'égard d'une personne ne peut être prise sur le seul fondement d'un traitement automatisé des données destiné à définir le profil de l'intéressé ou à évaluer certains aspects de sa personnalité.

Les décisions prises dans le cadre de la conclusion ou de l'exécution d'un contrat et pour lesquelles la personne concernée a été mise à même de présenter ses observations et celles satisfaisant aux demandes de la personne concernée ne sont pas considérées comme issues d'un traitement automatisé.

Sous-section 2 : Des formalités préalables à la mise en œuvre des traitements des données personnelles

Article 78 : Les traitements automatisés des données font l'objet d'une déclaration auprès de l'APDPVP, à l'exception des traitements mentionnés aux articles 80, 81 et 82 ou à l'article 111 de la présente loi.

Article 79 : La déclaration des traitements automatisés des données comporte l'engagement que le traitement satisfait aux exigences de la loi.

Elle est adressée à l'APDPVP par tout moyen de communication laissant trace.

Le responsable du traitement est tenu de notifier sans délai excessif, à tout le moins à l'Autorité de contrôle compétente, les violations des données susceptibles de porter gravement atteintes aux droits et libertés fondamentaux des personnes concernées.

L'APDPVP délivre, sans délai et par tout moyen laissant trace, un récépissé.

Le demandeur peut mettre en œuvre le traitement dès réception de ce récépissé.

La demande de récépissé doit être renouvelée à l'expiration de sa validité suivant les dispositions du règlement intérieur.

Les traitements relevant d'un même responsable de traitement et ayant des finalités identiques ou liées entre elles peuvent faire l'objet d'une déclaration unique. Dans ce cas, les informations requises, en application de l'article 80 ci-dessous, ne sont fournies pour chacun des traitements que dans la mesure où elles lui sont propres.

Article 80 : Pour les catégories les plus courantes de traitements des données dont la mise en œuvre n'est pas susceptible de porter atteinte à la vie privée ou aux libertés, l'Autorité établit et publie des normes, après avoir reçu, le cas échéant, les propositions formulées par le responsable de traitement à simplifier l'obligation de déclaration, notamment, les organismes, associations religieuses, philosophiques, politiques ou syndicales à but non lucratif.

Ces normes précisent :

-les finalités des traitements faisant l'objet d'une déclaration simplifiée ;
-les données ou catégories des données traitées ;
-la ou les catégories des personnes concernées ;
-les destinataires ou catégories des destinataires auxquels les données sont communiquées ;

-la durée de conservation des données.

Les traitements qui correspondent à l'une de ces normes font l'objet d'une déclaration simplifiée de conformité obligatoire auprès de l'APDPVP.

L'APDPVP peut définir, parmi les catégories de traitements mentionnés à l'alinéa 1er, celles qui, compte tenu de leurs finalités, de leurs destinataires ou catégories de destinataires, des données traitées, de la durée de conservation de celles-ci et des catégories de personnes concernées, sont dispensées de déclaration.

Dans les mêmes conditions, l'Autorité peut autoriser les responsables de certaines catégories de traitements à procéder à une déclaration unique selon les dispositions du dernier alinéa de l'article 77 ci-dessus.

Article 81 : Sont mis en œuvre après autorisation de l'APDPVP, à l'exclusion de ceux qui sont mentionnés aux articles 81 et 82 de la présente loi :

-les traitements, automatisés ou non, mentionnés à l'article 74 de la présente loi ;
-les traitements automatisés portant sur des données génétiques, à l'exception de ceux d'entre eux qui sont mis en œuvre par des médecins ou des biologistes et qui sont nécessaires aux fins de la médecine préventive, des diagnostics médicaux ou de l'administration de soins ou de traitements ;
-les traitements, automatisés ou non, portant sur des données relatives aux infractions, condamnations ou mesures de sûreté, sauf ceux qui sont mis en œuvre par les auxiliaires de justice pour les besoins de leurs missions de défense des personnes concernées ;
-les traitements automatisés susceptibles, du fait de leur nature, de leur portée ou de leurs finalités, d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat en l'absence de toute disposition législative ou réglementaire ;
-l'interconnexion de fichier relevant d'une ou de plusieurs personnes morales gérant un service public et dont les finalités correspondent à des intérêts publics différents ;
-l'interconnexion de fichiers relevant d'autres personnes et dont les finalités principales sont différentes ;
-les traitements portant sur des données parmi lesquelles figure le numéro d'inscription des personnes dans un fichier national d'identification des personnes physiques et ceux qui requièrent une consultation de ce fichier sans inclure le numéro d'inscription des personnes à ce fichier ;
-les traitements automatisés des données comportant des appréciations sur les difficultés sociales des personnes ;
-les traitements automatisés comportant des données biométriques nécessaires au contrôle de l'identité des personnes.

Aux fins d'application du présent article, les traitements qui répondent à une même finalité, portent sur des catégories des données identiques et ont les mêmes destinataires ou catégories de destinataires peuvent être autorisés par une décision unique de l'APDPVP.

Dans ce cas, le responsable de chaque traitement adresse à l'APDPVP un engagement de conformité de celui-ci à la description figurant dans l'autorisation.

L'APDPVP se prononce dans un délai de deux mois à compter de la réception de la demande. Toutefois, ce délai peut être renouvelé une fois sur décision motivée de son Président. Lorsque l'APDPVP ne s'est pas prononcée dans ces délais, la demande d'autorisation est réputée rejetée.

Article 82 : Sont autorisés par arrêté du ou des ministres compétents, pris après avis de l'APDPVP, les traitements des données mis en œuvre pour le compte de l'Etat et :

-qui intéressent la sûreté de l'Etat, la défense ou la sécurité publique ;
-qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté.

L'avis de l'APDPVP est publié avec l'arrêté autorisant le traitement.

Certains traitements mentionnés au présent article peuvent être dispensés, par décret pris en Conseil des Ministres, de la publication de l'acte réglementaire qui les autorise ; pour ces traitements, est publié, en même temps que le décret autorisant la dispense de publication de l'acte, le sens de l'avis émis par l'APDPVP.

Pour l'application du présent article, les traitements qui répondent à une même finalité, portent sur des catégories des données identiques et ont les mêmes destinataires ou catégories de destinataires peuvent être autorisés par un acte réglementaire unique.

Dans ce cas, le responsable de chaque traitement adresse à l'APDPVP un engagement de conformité de celui-ci, à la description figurant dans l'autorisation.

Article 83 : Sont autorisés par décret pris en Conseil des Ministres, après avis de l'Autorité :

-le traitement des données mis en œuvre pour le compte de l'Etat, d'une personne morale de droit public ou d'une personne morale de droit privé gérant un service public, qui porte sur des données parmi lesquelles figure le numéro d'inscription des personnes dans un fichier national d'identification des personnes physiques ;

-le traitement des données mis en œuvre pour le compte de l'Etat, qui porte sur les données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes.

Article 84 : Sont autorisés par arrêté ou, en cas de traitement opéré pour le compte d'un établissement public ou d'une personne morale de droit privé gérant un service public, par décision de l'organe délibérant chargé de leur organisation, pris après avis de l'APDPVP :

-le traitement mis en œuvre par l'Etat ou les personnes morales mentionnées au premier alinéa de l'article 80 ci-dessus, qui requiert une consultation dans un fichier national d'identification des personnes physiques sans inclure le numéro d'inscription à ce fichier ;
-ceux des traitements mentionnés au premier alinéa de l'article 80 qui :

-ne comportent aucune des données sensibles ni celles mentionnées à l'article 74 ci-dessus ;
-ne donnent pas lieu à une interconnexion entre des traitements ou fichiers correspondant à des intérêts publics différents ;
-sont mis en œuvre par des services ayant pour mission, soit de déterminer les conditions d'ouverture ou l'étendue d'un droit des administrés, soit d'établir l'assiette, de contrôler ou de recouvrer des impositions ou taxes de toute nature, soit d'établir des statistiques ;

-le traitement relatif au recensement de la population ;
-le traitement mis en œuvre par l'Etat ou les personnes morales mentionnées au premier alinéa de l'article 80 ci-dessus aux fins de mettre à la disposition des usagers de l'administration un ou plusieurs télé-services de l'administration électronique, si ce traitement comporte des données parmi lesquelles figure le numéro d'inscription des personnes dans un fichier national d'identification ou tout autre identifiant des personnes physiques.

Les dispositions du dernier alinéa de l'article 81 ci-dessus sont applicables aux traitements relevant du présent article.

Article 85 : L'APDPVP, saisie dans le cadre des articles 81 et 82 de la présente loi, se prononce dans un délai de deux mois à compter de la réception de la demande. Toutefois, ce délai peut être renouvelé une fois sur décision motivée du président de l'APDPVP.

L'avis motivé demandé à l'APDPVP par les pouvoirs publics sur un traitement, qui n'est pas rendu à l'expiration du délai prévu au 1er alinéa, est réputé favorable.

Pour les responsables de traitements et les personnes morales privées, l'APDPVP se prononce dans un délai de deux mois à compter de la réception de la demande.

Toutefois, ce délai peut être renouvelé une fois sur décision motivée de son Président. Passé ce délai, la demande est réputée rejetée.

Article 86 : Les actes autorisant la création d'un traitement en application des articles 81, 82 et 83 de la présente loi précisent :

-la dénomination et la finalité du traitement ;
-le service auprès duquel s'exerce le droit d'accès défini au chapitre II de la présente loi ;
-les catégories des données enregistrées ;
-les destinataires ou catégories de destinataires habilités à recevoir communication de ces données ;
-le cas échéant, les dérogations à l'obligation d'information.

En matière de transaction électronique, si la collecte de l'identité du titulaire de la carte n'est pas nécessaire à la transaction, elle ne doit pas être collectée.

Un e-commerçant ne peut demander la transmission d'une copie de la carte de paiement même si le cryptogramme visuel et une partie des numéros sont masqués.

Article 87 : Les déclarations, demandes d'autorisation et demandes d'avis adressées à l'Autorité en vertu des dispositions de la présente section précisent :

-l'identité et l'adresse du responsable du traitement ou, si celui-ci n'est pas établi sur le territoire national, celle de son représentant et, le cas échéant, celle de la personne qui présente la demande ;
-la ou les finalités du traitement, ainsi que, pour les traitements relevant des articles 81, 82 et 83 de la présente loi, la description générale de ses fonctions ;
-le cas échéant, les interconnexions, les rapprochements ou toutes autres formes de mise en relation avec d'autres traitements ;
-les données traitées, leur origine et les catégories de personnes concernées par le traitement ;
-la durée de conservation des informations traitées ;
-le ou les services chargés de mettre en œuvre le traitement ainsi que, pour les traitements relevant des articles 80, 81 et 82, les catégories de personnes qui, en raison de leurs fonctions ou pour les besoins du service, ont directement accès aux données enregistrées ;
-les destinataires ou catégories de destinataires habilités à recevoir communication des données ;
-la fonction de la personne ou le service auprès duquel s'exerce le droit d'accès prévu au chapitre III de la présente loi, ainsi que les mesures relatives à l'exercice de ce droit ;
-les dispositions prises pour assurer la sécurité des traitements et des données et la garantie des secrets

protégés par la loi et, le cas échéant, l'indication du recours à un sous-traitant ;
-le cas échéant, les transferts de données envisagés à destination d'un Etat non membre d'une organisation sous-régionale et régionale n'assurant pas un niveau de protection suffisant, sous quelque forme que ce soit, à l'exclusion des traitements qui ne sont utilisés qu'à des fins de transit.

Les demandes d'avis portant sur les traitements intéressant la sûreté de l'Etat, la défense ou la sécurité publique peuvent ne pas comporter tous les éléments d'information énumérés ci-dessus.

Un décret, pris après avis de l'Autorité, fixe la liste des traitements et des informations que les demandes d'avis doivent comporter.

Le responsable d'un traitement déjà déclaré ou autorisé informe sans délai l'Autorité :

-de tout changement affectant les informations mentionnées au premier alinéa de l'article 78 de la présente loi ;
-de toute suppression du traitement.

Article 88 : L'APDPVP met à la disposition du public, dans un format ouvert et aisément réutilisable, la liste des traitements automatisés ayant fait l'objet d'une des formalités prévues à la présente section.

Cette liste précise pour chacun de ces traitements :

-l'acte décidant la création du traitement ou la date de la déclaration de ce traitement ;
-la dénomination et la finalité du traitement ;
-l'identité et l'adresse du responsable du traitement ou celles de son représentant ;
-la fonction de la personne ou le service auprès duquel s'exerce le droit d'accès prévu à la section 1ère du chapitre III de la présente loi ;
-les catégories de données faisant l'objet du traitement, ainsi que les destinataires et catégories de destinataires habilités à en recevoir communication ;
-le cas échéant, les transferts de données envisagés à destination d'un Etat non membre d'une organisation sous régionale et régionale n'assurant pas un niveau de protection suffisant.

Article 89 : Ne sont soumis à aucune des formalités préalables prévues au présent chapitre :

-les traitements ayant pour seul objet, la tenue d'un registre qui, en vertu de dispositions législatives ou réglementaires, est destiné exclusivement à l'information du public et est ouvert à la consultation de celui-ci ou de toute personne justifiant d'un intérêt légitime ;
-les traitements mentionnés au 3ème tiret de l'article 75 de la présente loi ;
-les traitements pour lesquels le responsable a désigné un délégué à la protection des données chargé d'assurer, d'une manière indépendante, le respect des obligations prévues dans la présente loi, sont dispensés des formalités prévues par les articles 78 et 79 de la présente loi, sauf lorsqu'un transfert des données à destination d'un autre Etat est envisagé.

En cas de non-respect des dispositions de la présente loi, le responsable du traitement est enjoint par l'Autorité de procéder aux formalités prévues à la présente loi. En cas de manquement constaté à ses devoirs, le délégué est déchargé de ses fonctions sur demande ou après consultation de l'Autorité.

Le responsable d'un traitement des données qui n'est soumis à aucune des formalités prévues au présent chapitre, communique à toute personne qui en fait la demande, les informations relatives à ce traitement.

Article 90 : Les avis, décisions et recommandations de l'Autorité sont publiés dans un journal d'annonces légales.

Sous-section 3 : Des obligations incombant aux responsables du traitement des données personnelles

Paragraphe 1 : De l'obligation de transparence des informations et des communications et des modalités d'exercice des droits de la personne concernée

Article 91 : Le responsable du traitement prend des mesures appropriées pour fournir à la personne concernée les informations prévues par les articles 91 et 92 ci-dessous. Il procède à toute communication au titre des articles 42, 49 à 54 et 76.

L'information de la personne concernée doit être concise, transparente, compréhensible, aisément accessible et formulée en de termes clairs et simples, en particulier lorsqu'elle est destinée à un enfant.

Les informations sont fournies par écrit ou par d'autres moyens y compris, au besoin, par voie électronique. Lorsque la personne concernée en fait la demande, les informations peuvent être fournies oralement, à condition que son identité soit prouvée.

Article 92 : Le responsable du traitement facilite l'exercice des droits conférés à la personne concernée, au titre des articles 42 et 49 à 54.

Article 93 : Le responsable du traitement fournit à la personne concernée, des informations sur les mesures prises à la suite d'une demande formulée en application des articles 42 et 49 à 54 dans un délai qui ne peut être

supérieur à un mois, à compter de la réception de la demande.

Toutefois, ce délai peut être prolongé de deux mois, compte tenu de la complexité des informations sollicitées et du nombre de demandes. Le responsable du traitement informe la personne concernée de cette prolongation et des motifs du report dans un délai d'un mois, à compter de la réception de la demande.

Lorsque la personne concernée présente sa demande sous une forme électronique, les informations sont fournies dans la même forme, à moins qu'elle ne demande qu'il en soit autrement.

Article 94 : Si le responsable du traitement ne donne pas suite à la demande formulée par la personne concernée, il informe celle-ci au plus tard dans un délai d'un mois, à compter de la réception de la demande, des motifs de son inaction et de la possibilité d'introduire une réclamation auprès de l'APDPVP et le cas échéant, de former un recours juridictionnel.

Article 95 : Aucun paiement n'est exigé pour fournir les informations au titre des articles 97 et 98 et pour procéder à toute communication et prendre toute mesure sur le fondement des articles 43 et 50 à 55.

Toutefois, lorsque les demandes d'une personne concernée sont manifestement infondées ou excessives, notamment en raison de leur caractère répétitif, le responsable du traitement peut :

-exiger le paiement de frais raisonnables qui tiennent compte des coûts administratifs supportés pour fournir les informations, procéder aux communications ou prendre les mesures demandées ;
-refuser de donner suite à ces demandes. Dans ce cas, il lui incombe de démontrer le caractère manifestement infondé ou excessif de la demande.

Article 96 : Lorsque le responsable du traitement a des doutes raisonnables quant à l'identité de la personne physique présentant la demande visée aux articles 42 et 49 à 65 il peut demander que lui soient fournies des informations supplémentaires nécessaires à l'authentification de l'intéressé.

Article 97 : Les informations communiquées aux personnes concernées, peuvent être, au besoin, assorties d'icônes normalisées.

Article 98 : La personne auprès de laquelle sont recueillies des données la concernant est informée par le responsable du traitement ou son représentant, au moment de la collecte des données :

-de l'identité et des coordonnées du responsable du traitement et, le cas échéant, celles de son représentant ;
-des coordonnées du délégué à la protection des données, le cas échéant ;
-des finalités et de la base juridique du traitement ;
-des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers lorsque le traitement est fondé sur l'un des cas de licéité prévus par la présente loi ;
-des destinataires ou catégories de destinataires des données, s'ils existent ;
-des transferts des données envisagés à destination d'un autre Etat ou d'une organisation internationale ;
-de la durée de conservation des données ou, en cas d'impossibilité, des critères utilisés pour déterminer cette durée ;
-de l'existence des droits qu'elle tient des dispositions du chapitre III de la présente loi ;
-de la possibilité de retirer son consentement à tout moment, sans porter atteinte à la licéité du traitement fondé sur le consentement donné avant le retrait de celui-ci ;
-du droit d'introduire une réclamation auprès de l'APDPVP ;
-de l'existence d'une prise de décision automatisée, y compris un profilage et, au moins en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée ;
-des informations permettant de savoir si l'exigence de fourniture de données a un caractère réglementaire ou contractuel ou si elle conditionne la conclusion d'un contrat et si la personne concernée est tenue de fournir ces données ;
-des conséquences éventuelles en cas de non-fourniture des données.

Le responsable du traitement qui a l'intention d'effectuer un traitement ultérieur des données pour une finalité autre que celle sur le fondement de laquelle ces données ont été collectées, fournit au préalable à la personne concernée, des informations relatives à cette autre finalité.

Article 99 : Les dispositions de l'article 97 ci-dessus ne s'appliquent pas lorsque la personne concernée a déjà été informée.

Article 100 : Lorsque les données n'ont pas été collectées auprès de la personne concernée, le responsable du traitement fournit à l'intéressé les informations suivantes :

-l'identité et les coordonnées du responsable du traitement et, le cas échéant, celles du représentant du responsable du traitement ;
-les coordonnées du délégué à la protection des données, le cas échéant ;
-la finalité et la base juridique du traitement ;
-les catégories de données ;
-les destinataires ou les catégories de destinataires des données ;

-le transfert de données envisagé à destination d'un pays tiers ou une organisation internationale, le cas échéant ;
-la durée de conservation des données ou, en cas d'impossibilité, les critères utilisés pour déterminer cette durée ;
-les intérêts légitimes poursuivis par le responsable du traitement ou par un tiers ; à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée, lorsque celle-ci est un enfant ;
-l'existence des droits reconnus à la personne concernée visés au chapitre II de la présente loi ;
-la possibilité de retirer le consentement à tout moment, sans porter atteinte à la licéité du traitement fondé sur le consentement effectué avant le retrait de celui-ci ;
-le droit d'introduire une réclamation auprès de l'APDPVP ;
-l'origine des données et, le cas échéant, une mention indiquant qu'elles sont issues ou non de sources accessibles au public ;
-l'existence d'une prise de décision automatisée, y compris un profilage et, au moins en pareil cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée.

Article 101 : Le responsable du traitement fournit les informations prévues par l'article 100 ci-dessus :

-dans un délai ne dépassant pas un mois, eu égard aux circonstances particulières dans lesquelles les données sont traitées ;
-si les données doivent être utilisées aux fins de communication avec la personne concernée, au plus tard au moment de la première communication à ladite personne ;
-s'il est envisagé de communiquer les informations à un autre destinataire, au plus tard lorsque les données sont communiquées pour la première fois.

Article 102 : Lorsqu'il a l'intention d'effectuer un traitement ultérieur des données pour une finalité autre que celle sur le fondement de laquelle ces données ont été collectées, le responsable du traitement fournit au préalable à la personne concernée des informations relatives à cette autre finalité et toute autre information pertinente prévue par les articles 43 à 49 et 100.

Article 103 : Les dispositions des articles 54 à 99 ne s'appliquent pas lorsque :

-la personne concernée a déjà été informée ;
-la fourniture de telles informations se révèle impossible ou exigerait des efforts disproportionnés, en particulier pour le traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique, historique ou statistiques, et dans la mesure où l'obligation visée à l'article 97 est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs dudit traitement. En pareils cas, le responsable du traitement prend des mesures appropriées pour protéger les droits et libertés ainsi que les intérêts légitimes de la personne concernée.

Article 104 : Tout abonné ou utilisateur d'un service de communications électroniques doit être informé de manière claire et complète, par le responsable du traitement ou son représentant :

-de la finalité de toute action tendant à accéder, par voie de transmission électronique, à des informations déjà stockées dans son équipement terminal de communications électroniques, ou à inscrire des informations dans cet équipement ;
-des moyens dont il dispose pour s'y opposer.

Ces accès ou inscriptions ne peuvent avoir lieu qu'à condition que l'abonné ou la personne utilisatrice ait exprimé, après avoir reçu cette information, son accord qui peut résulter de paramètres appropriés de son dispositif de connexion ou de tout autre dispositif placé sous son contrôle.

Ces dispositions ne sont pas applicables si l'accès aux informations stockées dans l'équipement terminal de l'utilisateur a pour finalité exclusive de permettre ou faciliter la communication par voie électronique et, est strictement nécessaire à la fourniture d'un service de communication en ligne à la demande expresse de l'utilisateur.

Article 105 : Les données recueillies par les prestataires de services de certification électronique pour les besoins de délivrance et de conservation des certificats liés aux signatures électroniques, doivent l'être directement auprès de la personne concernée et ne peuvent être traitées que pour les fins en vue desquelles elles ont été recueillies, sauf consentement express de la personne concernée.

Article 106 : A titre de responsable de traitement ou de sous-traitant, un prestataire fournissant la signature électronique doit nécessairement garantir la confidentialité des données et la sécurisation de ses services informatiques ainsi que les droits d'accès, de modification et de suppression.

Article 107 : Lorsque peuvent être requis pour la mise en œuvre de la signature électronique, l'utilisation d'informations considérées comme données personnelles à savoir : les noms, prénoms ; adresses e-mail, numéros de téléphone, adresses postales. La mise en œuvre est subordonnée à l'adoption d'une norme simplifiée aux fins de signature électronique, de dépôt et de conservation des actes authentiques sur support électronique.

Article 108 : Lorsque les données recueillies sont appelées à faire l'objet, à bref délai, d'un procédé

d'anonymisation préalablement reconnu conforme aux dispositions de la présente loi par l'APDPVP, les informations délivrées par le responsable du traitement à la personne concernée peuvent se limiter à celles mentionnées au 1er et au 2nd tirets de l'article 98 ci-dessus.

Article 109 : Les dispositions de l'article 98 de la présente loi ne s'appliquent pas aux données recueillies dans les conditions prévues par cet article et utilisées lors d'un traitement mis en œuvre pour le compte de l'Etat et intéressant la sûreté de l'Etat, la défense, la sécurité publique ou ayant pour objet l'exécution de condamnations pénales ou de mesures de sûreté, dans le cas où une telle limitation est nécessaire au respect des fins poursuivies par le traitement.

Article 110 : Les dispositions de la présente sous-section ne s'appliquent pas aux traitements des données ayant pour objet la prévention, la recherche, la constatation ou la poursuite d'infractions pénales.

Paragraphe 2 : De l'obligation de confidentialité

Article 111 : Le traitement des données est confidentiel. Il est effectué par des personnes qui agissent sous l'autorité du responsable du traitement et seulement sur ses instructions.

Aux fins de réalisation du traitement, le responsable doit choisir des personnes présentant, au regard de la préservation de la confidentialité des données, toutes les garanties tant de connaissances techniques et juridiques que d'intégrité personnelle.

Un engagement écrit des personnes amenées à traiter de telles données à respecter la présente loi doit être signé.

Le non-respect de l'obligation de confidentialité dans le traitement des données constitue une violation du secret professionnel. A ce titre, il est passible des peines prévues par le Code Pénal.

Article 112 : Les données ne peuvent faire l'objet d'une opération de traitement de la part d'un sous-traitant, d'une personne agissant sous l'autorité du responsable du traitement ou de celle du sous-traitant, que sur instruction du responsable du traitement.

Le sous-traitant doit présenter des garanties suffisantes pour assurer la mise en œuvre des mesures de sécurité et de confidentialité mentionnées à l'article 111 ci-dessus.

Cette exigence ne décharge pas le responsable du traitement de son obligation de veiller au respect de ces mesures.

Le contrat liant le sous-traitant au responsable du traitement comporte l'indication des obligations incombant au sous-traitant en matière de protection, de sécurité et de confidentialité des données.

Paragraphe 3 : De l'obligation de sécurité

Article 113 : Le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, notamment :

-la pseudonymisation et le chiffrement des données ;
-les moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
-les moyens permettant de rétablir la disponibilité et l'accès aux données dans des délais appropriés, en cas d'incident physique ou technique ;
-la procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

Article 114 : Le responsable du traitement et le sous-traitant prennent des mesures afin de garantir que toute personne physique, agissant sous leur autorité, qui a accès à des données, ne les traite pas, excepté sur instruction du responsable du traitement.

Article 115 : Lorsqu'un traitement doit être effectué pour le compte d'un responsable du traitement, celui-ci fait uniquement appel à des sous-traitants qui présentent les garanties suffisantes, aux plans technique et organisationnel, afin d'assurer la protection des droits de la personne concernée.

Le sous-traitant ne peut recruter un autre sous-traitant qu'après autorisation écrite, spécifique ou générale, du responsable du traitement.

La relation entre le sous-traitant et le responsable du traitement est régi par un contrat ou tout autre acte juridique qui précise l'objet, la durée, la nature, la finalité du traitement, le type de données, les catégories de personnes concernées, les obligations et les droits du responsable du traitement.

Article 116 : Le contrat ou tout autre acte juridique, prévoit notamment que le sous-traitant :

-ne traite les données que sur instruction documentée du responsable du traitement, y compris lorsqu'il envisage un transfert de données vers un pays tiers ou une organisation internationale ;
-veille à ce que les personnes autorisées à traiter les données s'engagent à respecter les obligations de confidentialité ;
-prend toutes les mesures requises en vertu de l'article 111 de la présente loi ;

-respecte les conditions prévues par l'article 117 de la présente loi pour le recrutement d'un autre sous-traitant ;
tient compte de la nature du traitement et apporte son soutien au responsable du traitement à l'effet de s'acquitter de son obligation de donner suite aux demandes du droit d'accès prévu au chapitre II de la présente loi ;
-respecte les obligations concernant la sécurité du traitement, la notification à l'Autorité et la communication à la personne concernée d'une violation des données, l'analyse d'impact relative à la protection des données et la consultation préalable de l'APDPVP lorsque le traitement présente un risque élevé ;
-renvoie toutes les données au responsable du traitement ou les supprime au terme de la prestation de services ;
-met à la disposition du responsable du traitement toute information nécessaire attestant du respect des obligations prévues au présent article, en vue de la réalisation des audits et des inspections par le responsable du traitement ou d'un auditeur mandaté ;
-informe immédiatement, par tout moyen laissant trace, le responsable du traitement de la non-conformité d'une instruction à la présente loi.

Article 117 : Lorsqu'un sous-traitant recrute un autre sous-traitant pour mener des activités de traitement spécifiques pour le compte du responsable du traitement, les mêmes obligations en matière de protection des données que celles fixées dans le contrat ou dans un autre acte juridique entre le responsable du traitement et le sous-traitant s'appliquent à cet autre sous-traitant par contrat ou au moyen d'un autre acte juridique.

Lorsque cet autre sous-traitant ne remplit pas ses obligations en matière de protection des données, le sous-traitant initial demeure pleinement responsable de l'exécution par l'autre sous-traitant de ses obligations.

Le contrat ou l'autre acte juridique se présente sous forme écrite, y compris en format électronique.

Le responsable du traitement ainsi que le sous-traitant doivent prendre des mesures de sécurité appropriées contre l'accès accidentel ou non autorisé aux données à caractère personnelles, leur destruction, perte, utilisation, modification ou divulgation.

Il est tenu de notifier sans délai excessif, à tout le moins à l'APDPVP, les violations des données susceptibles de porter gravement atteintes aux droits et libertés fondamentaux des personnes concernées.

Paragraphe 4 : Des obligations de conservation et de pérennité

Article 118 : Le responsable du traitement est tenu de prendre toute mesure utile pour assurer la pérennité des données. Les données doivent être collectées pour des finalités déterminées, explicites et légitimes et ne peuvent pas être traitées ultérieurement de manière incompatible avec ses finalités.

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

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.

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

Paragraphe 5 : De l'obligation de tenir un registre des activités de traitement

Article 119 : Le responsable du traitement ou, le cas échéant, son représentant, tient un registre des activités de traitement effectuées sous sa responsabilité.

Ce registre comporte notamment les informations suivantes :

-le nom et les coordonnées du responsable du traitement et, le cas échéant, ceux du responsable conjoint du traitement, du représentant du responsable du traitement et du délégué à la protection des données ;
-les finalités du traitement ;
-la description des catégories de personnes concernées et des catégories de données collectées et traitées ;
-les catégories de destinataires auxquels les données ont été ou sont communiquées, y compris les destinataires dans des pays tiers ou des organisations internationales ;
-les transferts de données vers un pays tiers ou une organisation internationale, le cas échéant ;
-les délais prévus pour l'effacement des données, dans la mesure du possible ;
-la description générale des mesures techniques et organisationnelles mises en place.

Article 120 : Le sous-traitant ou, le cas échéant, son représentant, tient un registre comportant les informations relatives aux catégories d'activités de traitement effectuées pour le compte du responsable du traitement.

Ce registre comprend notamment les informations suivantes :

-le nom et les coordonnées du ou des sous-traitants du responsable du traitement pour le compte duquel le sous-traitant agit ainsi que, le cas échéant, les noms et les coordonnées du représentant du responsable du traitement ou de son sous-traitant et ceux du délégué à la protection des données ;
-les catégories de traitement effectuées pour le compte du responsable du traitement ;
-les transferts de données vers un pays tiers ou une organisation internationale, le cas échéant ;
-la description générale des mesures techniques et organisationnelles mises en place.

Article 121 : Les registres prévus par les articles 119 et 120 se présentent sous une forme écrite, y compris le format électronique.

Article 122 : Le responsable du traitement ou le sous-traitant et, le cas échéant, leurs représentants mettent le registre à la disposition de l'Autorité.

Article 123 : Les dispositions prévues par les articles 119 et 120 ne s'appliquent pas à une entreprise ou à une organisation comptant moins de 10 employés, sauf si le traitement effectué :

-présente des risques pour les droits et libertés des personnes concernées ;
-n'est pas occasionnel ;
-porte notamment sur les données sensibles, ou les données relatives aux condamnations aux infractions pénales.

Paragraphe 6 : De l'obligation de désigner un délégué à la protection des données personnelles et de la vie privée

Article 124 : Un délégué à la protection des données peut être désigné au sein ou en dehors des organismes publics ou privés.

Il peut s'agir des personnes physiques ou morales.

En cas de désignation d'une personne morale, elle doit répondre aux conditions suivantes :

-être une personne morale de droit Gabonais ;
-être à jour avec les impôts et les cotisations sociales ;
-exercer au moins depuis trois ans les activités dans le domaine du droit, de l'informatique et des télécommunications ;
-produire une police d'assurance couvrant les risques professionnels liés à l'activité de protection des données personnelles ;
-disposer de personnels ayant au moins le profil d'un délégué à la protection des données personnelles.

La personne morale peut être désignée par un ou plusieurs responsables de traitement et peut exercer ses missions auprès de ces derniers sous le contrôle de l'Autorité de Protection.

Les délégués à la protection des données sont agréés par l'APDPVP sur la base d'un cahier des charges et inscrits sur une liste d'aptitude.

Article 125 : Le responsable du traitement et le sous-traitant désignent un délégué à la protection des données lorsque :

-le traitement est effectué par une autorité publique ou un organisme public, à l'exception des juridictions agissant dans le cadre de l'exercice de leur fonction juridictionnelle ;
-les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées ;
-les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de données sensibles et de données relatives aux condamnations liées aux infractions pénales.

Article 126 : Un groupe d'entreprises peut désigner un seul délégué à la protection des données, qui doit être facilement joignable à partir de chaque lieu d'établissement.

Article 127 : Lorsque le responsable du traitement ou le sous-traitant est une autorité publique ou un organisme public, un seul délégué à la protection des données peut être désigné pour plusieurs autorités ou organismes publics.

Article 128 : Le responsable du traitement ou le sous-traitant, les associations et les autres organismes représentant des catégories de responsables du traitement ou de sous-traitants différents de ceux prévus par l'article 125, peuvent désigner un délégué à la protection des données qui veille à la mise en œuvre de la présente loi.

Article 129 : Le délégué à la protection des données peut être un membre du personnel du responsable du traitement ou du sous-traitant, ou exercer ses missions sur la base d'un contrat de service.

Article 130 : Le délégué à la protection des données est désigné sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de

sa capacité à accomplir les missions prévues par l'article 138 ci-dessous.

Article 131 : Le responsable du traitement ou le sous-traitant notifie la désignation du délégué à la protection des données à l'APDPVP.

Article 132 : Le délégué à la protection des données est associé à toutes les questions relatives à la protection des données.

Article 133 : Le responsable du traitement et le sous-traitant mettent à la disposition du délégué à la protection des données personnelles les ressources nécessaires à la réalisation des missions prévues par l'article 138, permettant à ce dernier d'apprécier les conditions de mise en œuvre des traitements, en lui facilitant l'accès aux données et aux opérations de traitement.

Le responsable du traitement et le sous-traitant aident le délégué à exercer les missions prévues par l'article 140 ci-dessous en lui fournissant les ressources nécessaires à l'exercice de ses missions ainsi que l'accès aux données et aux opérations de traitement, tout en lui permettant d'entretenir ses connaissances spécialisées.

Article 134 : Le délégué à la protection des données dispose d'une liberté d'organisation de son champ d'action, sous l'autorité du responsable du traitement ou sous celle du sous-traitant. Il ne peut être relevé de ses fonctions ou pénalisé par le responsable du traitement ou par le sous-traitant pour l'exercice de ses missions qu'après avis de l'APDPVP.

Le délégué à la protection des données présente son rapport au niveau le plus élevé de la direction du responsable du traitement ou du sous-traitant.

Article 135 : Le délégué à la protection des données reçoit les requêtes des personnes concernées pour toutes les questions relatives au traitement de leurs données et à l'exercice des droits que leur confère la présente loi.

Article 136 : Le délégué à la protection des données est soumis au secret professionnel et à l'obligation de confidentialité dans le cadre de l'exercice de ses missions.

Article 137 : Le délégué à la protection des données peut se voir confier par le responsable du traitement ou le sous-traitant, des missions et des taches autres que celles relevant de son domaine de compétence. Dans ce cas, le responsable du traitement ou le sous-traitant veille à ce que ces autres missions et ces tâches n'entraînent pas de conflit d'intérêts.

Article 138 : Le délégué à la protection des données est responsable de la conformité du traitement des données. Ses missions couvrent l'ensemble des traitements mis en œuvre par l'organisme qui l'a désigné.

À ce titre, il est notamment chargé :

-d'informer et conseiller le responsable du traitement ou le sous-traitant, ainsi que les personnes de l'organisme qui procèdent au traitement des données sur les obligations qui leur incombent, en vertu de la présente loi ;
-de contrôler le respect de la présente loi et des règles internes mises en place par le responsable du traitement ou le sous-traitant en matière de protection de données y compris la répartition des responsabilités, la sensibilisation et la formation du personnel qui participent aux opérations de traitement et d'audits ;
-de rendre un avis sur les études d'analyse d'impact relative à la protection des données et de vérifier l'exécution de celle-ci ;
-de coopérer avec l'APDPVP, y compris en cas de consultation préalable par le responsable du traitement lorsqu'une analyse d'impact relative à la protection des données est effectuée et de mener des consultations, le cas échéant, sur tout autre sujet.

Article 139 : Le délégué à la protection des données est le point focal entre l'APDPVP et le responsable du traitement ou le sous-traitant qui l'a désigné.

À ce titre, il est notamment chargé d'organiser des formations concernant le traitement des données au sein de l'organe et de tenir un registre du traitement des données personnelles du responsable du traitement ou le sous-traitant.

Article 140 : Le délégué dispose, pour garantir l'effectivité de ses missions, d'un bureau, des moyens matériels, organisationnels et des ressources suffisantes lui permettant d'exercer ses missions.

Les missions du délégué à la protection des données prennent fins en cas de :

-manquement à ses missions constaté par le responsable de traitement et signalé à l'Autorité ;
-démission ;
-décision de remplacement prise par le responsable de traitement ;
-faillite, liquidation ou redressement judiciaire ;
-décès ou indisponibilité permanente ;
-rupture du lien contractuel avec le responsable de traitement.

Article 141 : Le délégué à la protection des données tient compte, dans l'accomplissement de ses missions, du risque associé aux opérations de traitement, en raison de la nature, de la portée, du contexte et des finalités du traitement.

Dans l'exercice de ses fonctions, le délégué à la protection des données personnelles jouit de la même protection que les représentants du personnel.

Article 142 : En cas de violation de données, le responsable du traitement informe, sans délai, l'APDPVP.

Cette information porte sur :

-la nature de la violation des données y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation, les catégories et le nombre approximatif d'enregistrements de données concernées ;
-le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
-les conséquences probables de la violation de données ;
-les mesures prises ou celles que le responsable du traitement se propose de prendre pour remédier à la violation des données, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Article 143 : Le responsable du traitement accompagne la note d'information de toute pièce probante justifiant de la violation des données.

Article 144 : Le sous-traitant notifie, sans délai, au responsable du traitement toute violation de données dès qu'il en a pris connaissance.

Article 145 : Lorsqu'une violation de données est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement informe la personne concernée dans les meilleurs délais.

Article 146 : La communication à la personne concernée visée à l'article 145 ci-dessus décrit, en des termes clairs et simples, la nature de la violation de données et contient au moins les informations et mesures visées à l'article 142.

Article 147 : La communication à la personne concernée visée à l'article 145 n'est pas nécessaire si l'un des cas suivants se présente :

-le responsable du traitement a pris et mis en œuvre les mesures de protection des données affectées par la violation ;
-le responsable du traitement a pris des mesures préventives contre tout risque élevé pour les droits et libertés des personnes concernées ;
-le responsable du traitement constate que la communication exige des efforts disproportionnés. Il procède alors à une communication publique ou prend une mesure similaire permettant aux personnes concernées d'être informées de manière tout aussi efficace ;

Si le responsable du traitement n'a pas déjà communiqué aux personnes concernées la violation de leurs données la concernant, l'APDPVP peut, après avoir examiné la gravité de la violation, mettre en demeure le responsable du traitement d'informer également les intéressés.

Chaque responsable de traitement tient à jour un registre des violations de données, qui mentionne notamment leurs modalités, leur incidence et les mesures prises pour y remédier. Il le tient, à toutes fins utiles, à la disposition de l'APDPVP.

Chapitre IV : Des principes spécifiques relatifs au traitement de certaines catégories des données personnelles et de la vie privée

Section 1 : Du traitement des données personnelles relatif à la recherche dans le domaine de la santé

Article 148 : Le traitement des données personnelles aux fins de recherche dans le domaine de la santé est soumis aux dispositions de la présente loi.

Article 149 : Sont exclus du champ d'application des dispositions du présent chapitre :

-le traitement des données personnelles ayant pour fin le suivi thérapeutique ou médical individuel des patients ;
-le traitement permettant d'effectuer des études à partir des données ainsi recueillies si ces études sont réalisées par les personnels assurant ce suivi et destinées à leur usage exclusif.

Article 150 : Le traitement de données personnelles ayant une finalité d'intérêt public de recherche, d'étude ou d'évaluation est autorisé par l'APDPVP, dans le respect des principes définis par la présente loi.

L'APDPVP prend sa décision après avis d'un comité consultatif sur le traitement de l'information en matière de recherche.

Article 151 : Pour chaque demande de mise en œuvre d'un traitement des données, un comité consultatif sur le traitement de l'information en matière de recherche dans le domaine de la santé, institué auprès du Ministre chargé de la recherche et composé de personnes compétentes en matière de recherche dans le domaine de la santé, d'épidémiologie, de génétique et de bio-statistique, émet un avis sur la méthodologie de la recherche au regard des dispositions de la présente loi, la nécessité du recours à des données et la pertinence de celles-ci par rapport à l'objectif de la recherche, préalablement à la saisine de l'Autorité.

Le comité consultatif dispose d'un mois pour transmettre son avis au demandeur. A défaut, l'avis est réputé favorable. En cas d'urgence, ce délai peut être ramené à quinze jours.

Le Président du comité consultatif peut mettre en œuvre une procédure simplifiée.

La mise en œuvre du traitement des données personnelles est ensuite soumise à l'autorisation de l'APDPVP, qui se prononce dans les conditions prévues par le tiret 2 de l'alinéa 1 de l'article 81 de la présente loi.

Pour les catégories les plus usuelles des traitements automatisés ayant pour finalité la recherche dans le domaine de la santé et portant sur des données ne permettant pas une identification directe des personnes concernées, l'Autorité peut homologuer et publier des méthodologies de référence, établies en concertation avec le comité consultatif ainsi qu'avec les organismes publics et privés représentatifs, et destinées à simplifier la procédure prévue aux quatre premiers alinéas du présent article.

Ces méthodologies précisent les normes auxquelles doivent correspondre les traitements pouvant faire l'objet d'une demande d'avis ou d'une demande d'autorisation simplifiées.

Pour le traitement qui correspond aux modalités fixées par une norme, seul un engagement de conformité valant formalité préalable est envoyé à l'APDPVP.

Pour les autres catégories de traitements, le comité consultatif fixe, en concertation avec l'Autorité, les conditions dans lesquelles son avis n'est pas requis.

Article 152 : Nonobstant les règles relatives au secret professionnel, les membres des professions de santé peuvent transmettre les données qu'ils détiennent dans le cadre d'un traitement des données autorisé en application de l'article 153 ci-dessous.

Lorsque ces données permettent l'identification des personnes, elles sont codées avant leur transmission. Toutefois, il peut être dérogé à cette obligation lorsque le traitement des données est associé à des études de pharmacovigilance ou à des protocoles de recherche réalisés dans le cadre d'études coopératives nationales ou internationales. Il peut également y être dérogé si une particularité de la recherche l'exige.

La demande d'autorisation comporte la justification scientifique et technique de la dérogation et l'indication de la période nécessaire à la recherche. A l'issue de cette période, les données sont conservées et traitées dans les conditions fixées par la présente loi.

La présentation des résultats du traitement des données ne peut en aucun cas permettre l'identification directe ou indirecte des personnes concernées.

Les données sont reçues par le responsable de la recherche désigné à cet effet par la personne physique ou morale autorisée à mettre en œuvre le traitement. Ce responsable veille à la sécurité des informations et de leur traitement, ainsi qu'au respect de la finalité de celui-ci.

Sous peine de poursuites pénales, les personnes appelées à mettre en œuvre le traitement des données ainsi que celles qui ont accès aux données sur lesquelles il porte, sont astreintes au secret professionnel.

Article 153 : Toute personne a le droit de s'opposer à ce que des données personnelles la concernant fassent l'objet de la levée du secret professionnel rendue nécessaire par un traitement de la nature de ceux qui sont prévus par l'article 109 de la présente loi.

Dans le cas où la recherche nécessite le recueil de prélèvements biologiques et express identifiants, le consentement éclairé et express des personnes concernées doit être obtenu préalablement à la mise en œuvre du traitement des données.

Les informations concernant les personnes décédées, y compris celles qui figurent sur les certificats de décès, peuvent faire l'objet d'un traitement des données, sauf si l'intéressé a, de son vivant, exprimé son refus par écrit.

Article 154 : Les personnes auprès desquelles sont recueillies des données ou à propos desquelles de telles données sont transmises sont, avant le début du traitement de ces données, individuellement informées :

-de la nature des informations transmises ;
-de la finalité du traitement des données ;
-des personnes physiques ou morales destinataires des données le cas échéant ;
-du droit d'accès institué à l'article 43 de la présente loi ;
-du droit d'opposition, de rectification et de suppression ou, de l'obligation de recueillir leur consentement.

Toutefois, ces informations peuvent ne pas être délivrées si, pour des raisons légitimes que le médecin traitant apprécie en conscience, le malade est laissé dans l'ignorance d'un diagnostic ou d'un pronostic grave.

Dans le cas où les données ont été initialement recueillies pour un autre objet que le traitement, il peut être dérogé à l'obligation d'information individuelle lorsque celle-ci se heurte à la difficulté de retrouver les personnes concernées.

Les dérogations à l'obligation d'informer les personnes de l'utilisation des données les concernant à des fins de recherche sont mentionnées dans le dossier de demande d'autorisation transmis à l'APDPVP, qui statue sur ce point.

Article 155 : Sont destinataires de l'information et exercent les droits prévus à l'article 43 de la présente loi, les titulaires de l'autorité parentale, pour les mineurs, ou le représentant légal pour les personnes faisant l'objet d'une mesure de tutelle ou de curatelle.

Article 156 : Toute information relative aux dispositions du présent chapitre doit être assurée dans tout établissement ou centre où s'exercent des activités de prévention, de diagnostic et de soins donnant lieu à la transmission de données, en vue d'un traitement mentionné à l'article 153 de la présente loi.

Article 157 : La mise en œuvre d'un traitement des données personnelles en violation des conditions prévues par le présent chapitre, entraîne le retrait temporaire ou définitif, de l'autorisation par l'APDPVP.

Il en est de même en cas de refus de se soumettre aux vérifications portant sur tous traitements diligentés par l'APDPVP, et de mettre à la disposition de celle-ci copies de tous documents ou supports d'informations utiles à ses missions.

Article 158 : La transmission vers un autre Etat des données non codées faisant l'objet d'un traitement ayant pour fin la recherche, l'étude ou l'évaluation dans le domaine de la santé n'est autorisée, que sous réserve du respect des règles énoncées au chapitre III de la présente loi.

Section 2 : Du traitement des données personnelles de santé à des fins d'évaluation ou d'analyse des pratiques ou activités de soins et de prévention

Article 159 : Le traitement de données personnelles de santé qui ont pour fin l'évaluation des pratiques de soins et de prévention sont autorisés dans les conditions prévues au présent chapitre.

Les dispositions du présent chapitre ne s'appliquent pas :

-aux traitements des données effectuées à des fins de remboursement ou de contrôle par les organismes chargés de la gestion d'un régime de base d'assurance maladie ;
-aux traitements effectués au sein des établissements de santé par les médecins responsables de l'information.

Article 160 : Les données issues des dossiers médicaux détenus dans le cadre de l'exercice libéral des professions de santé, ainsi que celles issues des systèmes d'information des caisses d'assurance maladie, ne peuvent être communiquées à des fins statistiques d'évaluation ou d'analyse des pratiques et des activités de soins et de prévention que sous la forme de statistiques agrégées ou de données par patient constituées de telle sorte que les personnes concernées ne puissent être identifiées.

Il ne peut être dérogé aux dispositions de l'alinéa précédent que sur autorisation de l'APDPVP. Dans ce cas, les données utilisées ne comportent ni les noms et prénoms des personnes concernées ni leur numéro d'inscription au fichier national d'identification des personnes physiques.

Article 161 : Pour chaque demande, l'APDPVP vérifie les garanties présentées par le demandeur pour l'application des dispositions de la présente loi et, le cas échéant, la conformité de sa demande à ses missions ou à son objet social.

L'APDPVP s'assure de la nécessité de recourir à des données et de la pertinence du traitement au regard de sa finalité déclarée d'évaluation ou d'analyse des pratiques ou des activités de soins et de prévention.

Elle vérifie que les données dont le traitement est envisagé ne comportent ni les noms et prénoms des personnes concernées ni leur numéro d'inscription au fichier national d'identification des personnes physiques.

En outre, si le demandeur n'apporte pas d'éléments suffisants pour attester la nécessité de disposer de certaines informations parmi l'ensemble des données dont le traitement est envisagé, l'APDPVP peut interdire la communication de ces informations par l'organisme qui les détient et n'autoriser le traitement que des données ainsi réduites.

L'APDPVP détermine la durée de conservation des données nécessaires au traitement et apprécie les dispositions prises pour assurer leur sécurité et la garantie des secrets protégés par la loi.

Article 162 : L'APDPVP, à compter de sa saisine par le demandeur, dispose d'un délai de deux mois pour se prononcer. Il peut être prorogé de deux mois.

A l'expiration de ce délai, le silence gardé par l'APDPVP vaut acceptation.

Les traitements répondant à une même finalité portant sur des catégories de données identiques et ayant des destinataires ou des catégories de destinataires identiques peuvent faire l'objet d'une décision unique de l'APDPVP.

Article 163 : Les traitements autorisés conformément aux articles 159 et 160 de la présente loi ne peuvent

servir à des fins de recherche ou d'identification des personnes.

Sous peine de poursuites pénales, les personnes appelées à mettre en œuvre ces traitements, ainsi que celles qui ont accès aux données ou aux résultats de ceux-ci et lorsqu'ils permettent indirectement d'identifier les personnes concernées, sont astreintes au secret professionnel.

Les résultats de ces traitements font l'objet d'une communication, d'une publication ou d'une diffusion que si l'identification des personnes sur l'état desquelles ces données ont été recueillies est impossible.

Section 3 : Du traitement des données personnelles aux fins de journalisme et d'expression littéraire et artistique

Article 164 : Les dispositions de la présente loi ne s'appliquent pas aux traitements de données mis en œuvre aux seules fins :

-d'expression littéraire et artistique ;
-d'exercice, à titre professionnel, de l'activité de journaliste, dans le respect des règles déontologiques de cette profession.

Article 165 : Pour les traitements mentionnés au 2ème tiret de l'article 164 ci-dessus, la dispense de l'obligation de déclaration prévue par l'article 89 de la présente loi est subordonnée à la désignation par le responsable du traitement d'un correspondant à la protection des données appartenant à un organisme de la presse écrite ou audiovisuelle. Celui-ci est chargé de tenir un registre des traitements mis en œuvre par ce responsable et d'assurer, d'une manière indépendante, l'application des dispositions de la présente loi.

Cette désignation est portée à la connaissance de l'APDPVP.

Article 166 : En cas de non-respect des dispositions des articles 164 et 165 de la présente loi, le responsable du traitement est enjoint par l'APDPVP de se mettre en conformité avec la loi.

En cas de manquement à ses obligations reposant sur des motifs réels et sérieux, le correspondant est déchargé de ses fonctions à la demande du responsable du traitement, après consultation de l'APDPVP.

Article 167 : Les dispositions de la présente loi ne font pas obstacle à l'application des dispositions des textes en vigueur, réprimant les infractions en matière de presse écrite, audiovisuelle ou en ligne.

Chapitre V : De l'interconnexion et du transfert des données personnelles et de la vie privée

Section 1 : De l'interconnexion des données personnelles

Article 168 : L'interconnexion des systèmes d'information prévus par les tirets 5 et 6 de l'article 81 de la présente loi relevant d'une ou de plusieurs personnes morales gérant un service public et dont les finalités correspondent à des intérêts publics différents fait l'objet d'une autorisation de l'APDPVP.

Il en est de même pour le traitement mis en œuvre par l'Etat aux fins de mettre à la disposition des usagers du service public un ou plusieurs services à distance dans le cadre de la numérisation de l'administration.

L'interconnexion de fichiers ne relevant de personnes privées et dont les finalités principales sont différentes est également soumise à autorisation de l'APDPVP.

Article 169 : La demande d'autorisation d'interconnexion prévue à l'article 81, tirets 5 et 6 de la présente loi comporte notamment les informations suivantes :

-la nature des données relative à l'interconnexion ;
-la finalité pour laquelle l'interconnexion est considérée nécessaire ;
-la durée pour laquelle l'interconnexion est permise ;
-les conditions et les termes de l'interconnexion au regard de la protection des données et de la vie privée.

L'interconnexion des systèmes d'information doit permettre d'atteindre des objectifs légaux ou statutaires présentant un intérêt légitime pour les responsables de traitement. Elle ne peut pas entraîner de discrimination de réduction des droits, libertés et garanties pour les personnes concernées ni être assortie de mesures de sécurité appropriées et doit tenir compte du principe de pertinence des données faisant l'objet de l'interconnexion.

L'autorisation peut être renouvelée par une demande des responsables du traitement.

Article 170 : Les demandes et les autorisations d'interconnexion sont inscrites sur le répertoire des traitements des données mis à la disposition du public.

Section 2 : Du transfert et du flux transfrontalier des données personnelles

Article 171 : Un responsable de traitement ne peut transférer des données personnelles vers un autre Etat que sur autorisation de l'APDPVP.

L'APDPVP doit garantir que cet Etat assure un niveau de protection suffisant de la vie privée, des libertés et droits fondamentaux des personnes à l'égard du traitement dont ces données font l'objet ou peuvent faire l'objet.

Le caractère suffisant du niveau de protection assuré par un Etat s'apprécie en fonction notamment des dispositions en vigueur dans cet Etat, des mesures de sécurité qui y sont appliquées, des caractéristiques propres au traitement, telles que ses fins et sa durée, ainsi que de la nature, de l'origine et de la destination des données traitées.

L'APDPVP publie la liste des Etats qui garantissent un niveau de protection suffisant à l'égard de tout transfert de données personnelles.

Article 172 : L'APDPVP peut exercer les pouvoirs prévus au présent chapitre à l'égard des traitements dont les opérations sont mises en œuvre, en tout ou partie, sur le territoire national, y compris lorsque le responsable du traitement est établi sur le territoire d'un autre Etat.

Article 173 : Le responsable d'un traitement peut transférer des données personnelles vers un Etat ne répondant pas aux conditions prévues à l'article 171 ci-dessus si la personne à laquelle se rapportent les données a consenti expressément à leur transfert et le transfert est nécessaire à l'une des conditions suivantes :

-à la sauvegarde de la vie de cette personne ;
-à la sauvegarde de l'intérêt public ;
-au respect d'obligations permettant d'assurer la constatation, l'exercice ou la défense d'un droit en justice ;
-à la consultation, dans des conditions régulières, d'un registre public qui, en vertu des dispositions législatives ou réglementaires, est destiné à l'information du public et est ouvert à la consultation de celui-ci ou de toute personne justifiant d'un intérêt légitime ;
-à l'exécution d'un contrat entre le responsable du traitement et l'intéressé, ou de mesures précontractuelles prises à la demande de celui-ci ;
-à la conclusion ou à l'exécution d'un contrat conclu ou à conclure, dans l'intérêt de la personne concernée, entre le responsable du traitement et un tiers.

Il peut également être fait exception à l'interdiction prévue à l'article 172 ci-dessus, par décision de l'APDPVP ou, s'il s'agit d'un traitement mentionné à l'article 84 de la présente loi, par décret pris après avis motivé et publié de l'APDPVP, lorsque le traitement garantit un niveau de protection suffisant de la vie privée ainsi que des libertés et droits fondamentaux des personnes, notamment en raison des clauses contractuelles ou règles internes dont il fait l'objet.

L'APDPVP porte à la connaissance des autres Etats, les décisions d'autorisation de transfert des données qu'elle prend au titre de l'alinéa précédent.

Article 174 : L'APDPVP délivre un récépissé avec mention de l'interdiction de procéder au transfert des données personnelles, lorsqu'elle constate qu'un Etat n'assure pas un niveau de protection suffisant à l'égard d'un transfert des données.

À cet effet, elle en informe sans délai les autorités officielles et le public.

L'APDPVP délivre un récépissé et enjoint au responsable du traitement, selon les cas, de suspendre ou d'annuler le transfert des données, lorsqu'elle est saisie d'une déclaration déposée en application de l'article 79 de la présente loi, faisant apparaître que des données seront transférées vers cet Etat.

L'APDPVP notifie au responsable du traitement la cessation de la suspension du transfert des données personnelles, lorsqu'elle constate que l'Etat vers lequel le transfert est envisagé assure désormais un niveau de protection suffisant.

Les flux transfrontaliers des données à caractère personnel entre responsable de traitement de données approuvés par une clause contractuelle, doivent garantir le respect des exigences relatives au transfert des données personnelles vers un tiers partie d'une institution régionale ou sous régionale intégrant la libre circulation des biens et des personnes.

Dans ce cas, les clauses contractuelles contiennent les normes de protection des données sur la base de la loi nationale.

Chapitre VI : De la protection des personnes concernées à l'égard de l'innovation technologique

Article 175 : L'Autorité de Protection veille au respect d'intérêt public, tel qu'un niveau élevé de la sécurité et des droits fondamentaux, assurant ainsi la protection des consommateurs, des droits des utilisateurs et de la vie privée.

À ce titre, la collecte, l'utilisation, la communication et le couplage des renseignements des personnes concernées, engendrés par le progrès technologique, notamment : les moteurs de recherche, les sites web, les plateformes, les applications en ligne, sont soumis à une mise en conformité définie par une norme.

Ils sont tenus au préalable de procéder aux formalités de déclaration auprès l'Autorité de Protection, avant toute exploitation de données personnelles et d'informations relatives à la vie privées en ligne.

Article 176 : Est considéré comme données personnelles ou données personnelles à l'ère numérique, toutes informations qui se rapportent à une personne adulte ou enfant. Il s'agit également de toutes les traces laissées par une personne sous une forme ou une autre, à chaque fois qu'elle entre en contact avec le monde numérique.

Section 1 : De l'innovation technologique

Article 177 : Les présentes dispositions visent à en cadrer l'Intelligence Artificielle de façon à la rendre digne de confiance, centré sur l'humain, l'éthique durable et inclusive.

Elles s'appliquent aux technologies d'Intelligence Artificielle conçues ou utilisés en République Gabonaise par tout opérateur traitant sur le marché.

Article 178 : Tous systèmes utilisant l'Intelligence Artificielle et qui inclus des données personnelles ou toutes informations relatives à la vie privée, doit faire l'objet d'un avis ou d'une déclaration et leurs modalités d'exploitation définies par une norme.

Article 179 : Lorsque des données personnelles ou des informations relatives à la vie privée constituent un ensemble de traces numériques qu'une personne ou une collectivité laisse sur internet, notamment : un pseudo, un nom, des images, des vidéos, des adresses IP, des favoris, des commentaires, constituent une identité numérique. Sa mise en exploitation est soumise à un avis ou à une autorisation délivrée par l'Autorité de Protection.

Article 180 : Toutes données personnelles ou informations relatives à la vie privée, incluses ou captées dans un système ou par un appareil notamment un drone, doit faire l'objet d'un avis ou d'une déclaration, leurs modalités d'exploitation définies par une norme.

Article 181 : Tout traitement de données personnelles ou d'informations relatives à la vie privée, contenu dans un système, une machine ou dans un objet connecté, est soumis à une déclaration et leurs modalités d'exploitation définies par une norme.

Article 182 : Tout traitement de données personnelles et ou d'informations relatives à la vie privée, inclus dans un système ou dans un environnement de reconnaissance faciale doit faire l'objet d'un avis ou d'une déclaration et leurs modalités d'exploitation définies par une norme.

Article 183 : Toute collecte, utilisation des données personnelles et ou toutes informations relatives à la vie privée dans un dispositif ou un système de vidéoprotection, vidéosurveillance, télévidéosurveillance ainsi que la télémédecine, doit faire l'objet d'une déclaration et leurs modalités d'exploitation définies par une norme.

Article 184 : Lorsque les données personnelles d'une personne physique par un dispositif permettent, de vérifier l'origine d'une information, de l'authentifier par signature électronique, leurs traitements font l'objet de déclaration et leurs modalités définies par une norme.

Article 185 : Tout traitement des données personnelles relatif à l'inscription dans un registre national à l'identification au sein d'un système d'information national, notamment un identifiant unique public, doit requérir l'avis préalable de l'APDPVP.

Article 186 : Les données personnelles inscrites au registre d'un secteur d'activité de traitement, contenu dans un numéro d'identification et attribué à une personne au sein d'un système d'information spécifique, est considéré comme identifiant sectoriel. Son traitement est soumis à une mise en conformité préalable auprès de l'Autorité de Protection des Données Personnelles et de la Vie Privée.

Article 187 : Les Plateformes web de gestion, utilisateurs de données personnelles et ou d'informations relatives à la vie privée doivent faire l'objet de mise en conformité auprès de l'Autorité.

Section 2 : De la protection de l'enfance

Article 188 : Au sens de la présente loi, conformément aux dispositions de l'article 1er de la Convention Internationale relative aux Droits des Enfants, un enfant s'entend de tout être humain âgé de moins de dix-huit ans, sauf si la majorité est atteinte plus tôt en vertu de la législation qui lui est applicable.

Article 189 : Nul enfant ne fera l'objet d'immixtion arbitraire ou illégale dans sa vie privée y compris en ligne, sa famille, son domicile ou sa correspondance, ni d'atteinte illégale à son honneur ainsi qu'à sa réputation sur internet.

Sous-section 1 : De la collecte et de l'exploitation

Article 190 : Toute collecte et traitement de données personnelles des enfants par des responsables de traitement notamment : les moteurs de recherches, les sites web, les platesformes, dans le cadre d'un service proposé sur internet, à travers des applications et services connectés téléchargés ainsi que la géolocalisation, n'est licite qu'à la condition d'avoir obtenue l'accord préalable de leurs parents ou de la personne qui exerce la responsabilité parentale.

Article 191 : Toute collecte de données personnelles et d'informations relatives à la vie privée des enfants recueillies de manière trompeuse et transmis à des tiers

sans le consentement éclairé préalable de l'autorité parentale, est interdit et sanctionné conformément à la présente loi et sans préjudice des autres lois en vigueur.

Article 192 : Les informations destinées aux enfants doivent être rédigées en des termes qui soient facilement compréhensibles par eux et donc adaptées à leur niveau de compréhension et à leurs capacités.

Article 193 : Le profilage des enfants est interdit, sauf conditions exceptionnelles liées à l'intérêt supérieur de l'enfant ou à des motifs d'intérêt public, après avis motivé ou autorisation de l'APDPVP.

Article 194 : Sans préjudice d'autres dispositions en vigueur en la matière, tout contrat passé par un enfant dans le cadre d'un service proposé sur internet est déclaré comme nul, dès lors qu'il lui porte préjudice.

Une demande devant la justice compétente, évalue les conséquences pour l'enfant.

Sous-section 2 : Des obligations spécifiques des fournisseurs de services en ligne

Article 195 : Tout responsable de traitement, fournisseurs de service en ligne, applications, sites web et platesformes destinés aux enfants est tenu d'inclure dans la conception de ses programmes, les mesures techniques nécessaires de protection et de confidentialité des données et des informations relatives à la vie privée telles que des systèmes de marquage et de filtrage.

Article 196 : Tout responsable de traitement, fournisseurs de service en ligne, doit établir une distinction claire entre la publicité, le divertissement et les jeux divers, ainsi que, lorsque l'utilisateur est susceptible de conclure une convention par le biais de l'Internet.

Article 197 : Tout responsable de traitement, fournisseurs de services en ligne doit établir une distinction claire entre le marketing visant les enfants et le marketing de biens et services uniquement destinés aux adultes.

Article 198 : Pour la sauvegarde de la vie privée des enfants, les annonces publicitaires ou la publicité visant les enfants sur internet par les fournisseurs de services en ligne, ne doit avoir d'effet dommageable pour ces derniers. À ce titre, les fournisseurs de services en ligne ne doivent exhorter les enfants à acheter des biens ou à conclure des conventions par le biais de l'Internet.

Article 199 : Les fournisseurs de services en ligne ne doivent inclure dans les sites web des lots, récompenses, conçus pour inciter les enfants à rester sur le site ou à prendre part à des activités. De même, il leur est interdit de ne pas inclure des liens vers d'autres sites web non conformes à leurs requêtes.

Chapitre VII : Du recours, du contrôle et des sanctions

Section 1 : Du recours

Article 200 : Toute personne a le droit de disposer d'un recours non juridictionnel et juridictionnel en cas de violation ou d'atteinte à sa personnalité en matière de données personnelles, conformément aux textes en vigueur.

L'APDPVP n'est pas compétente pour accorder une indemnisation aux personnes concernées ayant subi un préjudice en cas de violation ou d'atteintes de ses données personnelles. Pour toutes indemnisations, la personne concernée doit saisir les tribunaux de droit commun qui statuent sur l'existence et l'évaluation du préjudice.

Section 2 : Du contrôle de la mise en œuvre des traitements

Article 201 : Les membres de l'APDPVP ainsi que les agents de service assermentés et habilités ont accès, pour l'exercice de leurs missions, aux lieux, locaux, enceintes, installations ou établissements servant à la mise en œuvre d'un traitement des données personnelles et qui sont à usage professionnel, à l'exclusion des parties de ceux-ci affectées au domicile privé.

Les agents cités à l'alinéa 1er ci-dessus sont accompagnés d'Officiers de Police Judiciaire lors des missions de contrôle.

Le Procureur de la République territorialement compétent en est préalablement informé.

En cas d'opposition du responsable des lieux, la visite ne peut se dérouler qu'avec l'autorisation du Président du tribunal dans le ressort duquel sont situés les locaux à visiter ou du juge délégué par lui.

Le Président du tribunal est saisi à la requête du Président de l'APDPVP. Il statut par une ordonnance motivée.

Article 202 : Les membres de l'APDPVP et les agents peuvent demander communication de tous documents nécessaires à l'accomplissement de leur mission, quel qu'en soit le support et en prendre copie.

Ils peuvent recueillir, sur place ou sur convocation, tout renseignement et toute justification utile, accéder aux programmes informatiques, aux données et demander la transcription de tout traitement dans des documents appropriés directement utilisables pour les besoins du contrôle.

Les commissaires et les agents assermentés et habilités peuvent être assistés, lors des missions de contrôle, par des experts choisis par l'APDPVP.

Il est dressé contradictoirement un procès-verbal des vérifications et visites menées en application des articles ci-dessus.

Section 3 : Des sanctions

Sous-section 1 : Des sanctions administratives

Article 203 : L'Autorité apprécie et prononce sans graduation, selon le manquement constaté à la présente loi, les mesures ou les sanctions 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 constatés dans le délai qu'elle fixe ;
-une sanction pécuniaire.

Sous-section 2 : Des sanctions pécuniaires

Article 204 : Si le responsable du traitement ne se conforme pas à la mise en demeure qui lui a été adressée, il peut faire l'objet d'une convocation par audition. Après débat contradictoire, l'Autorité pour la Protection des Données Personnelles et de la Vie Privée peut prononcer à son encontre les sanctions suivantes :

-suspension provisoire de collecter et de traiter les données personnelles pour une durée de trois mois à l'expiration de laquelle, la suspension devient définitive ;
-amende de un million à cent millions de Francs CFA.

Le montant de la sanction pécuniaire prévue à l'alinéa ci-dessus est proportionné à la gravité des manquements commis et aux avantages tirés de ce manquement.

Lors du premier manquement, il ne peut excéder quatre-vingt-dix-huit millions quatre cent mille francs CFA. En cas de récidive, il ne peut excéder trois cent millions de francs CFA ou, s'agissant d'une entreprise, 5% du chiffre d'affaires hors taxes du dernier exercice clos dans la limite de cent quatre-vingt-seize millions de francs CFA.

Lorsque l'APDPVP a prononcé une sanction pécuniaire devenue définitive avant que le juge pénal ait statué définitivement sur les mêmes faits ou des faits connexes, celui-ci peut ordonner que la sanction pécuniaire s'impute sur l'amende qu'il prononce.

Le recouvrement des pénalités se fait conformément à la législation relative au recouvrement des créances de l'Etat en matière d'impôts.

Article 205 : L'APDPVP peut rendre publics les avertissements qu'elle prononce. Elle peut également, en cas de mauvaise foi du responsable du traitement, ordonner l'insertion des sanctions qu'elle prononce dans une publication, journaux et supports qu'elle désigne. Les frais sont supportés par les personnes sanctionnées.

Article 206 : Un responsable de traitement qui dispose d'un récépissé de déclaration ou d'une autorisation et qui ne respecte pas les obligations découlant de la présente loi encourt, après mise en demeure, l'une des sanctions suivantes :

-la suspension du récépissé ou de l'autorisation pour une durée n'excédant pas deux mois ;
-le retrait définitif du récépissé ou de l'autorisation à l'expiration du délai de suspension ;
-une amende de un million à cent millions de francs CFA.

L'amende est proportionnelle à la gravité du manquement et aux avantages qui en sont tirés.

Article 207 : Un responsable de traitement qui ne dispose pas d'un récépissé de déclaration ou d'une autorisation est un responsable de traitement de fait.

Ce dernier encourt une amende d'un montant de un million à cent millions de francs CFA, assortie d'une mise en demeure portant régularisation dans un délai fixé par l'Autorité.

Sous-section 3 : Des sanctions d'urgence

Article 208 : L'APDPVP peut, lorsqu'elle constate que la mise en œuvre d'un traitement ou l'exploitation des données entraînent une violation de droits et libertés, prononcer :

-l'interruption de la mise en œuvre du traitement pour une durée maximale de trois mois ;
-le verrouillage de certaines données traitées pour une durée maximale de trois mois ;
-l'interdiction temporaire du traitement pour une période n'excédant pas trois mois ;
-l'interdiction définitive d'un traitement contraire aux dispositions de la présente loi.

Article 209 : L'APDPVP peut, à la demande d'une autorité exerçant des compétences analogues, procéder à des vérifications dans les conditions prévues à la section I du présent chapitre, sauf s'il s'agit d'un traitement mentionné à l'article 83.

L'APDPVP est habilitée à communiquer les informations qu'elle recueille ou qu'elle détient, à leur demande, aux autorités exerçant des compétences analogues.

Article 210 : Les sanctions et les décisions prises par l'Autorité sont susceptibles de recours devant le Conseil d'Etat, conformément aux dispositions des textes en vigueur.

Article 211 : Toute personne concernée peut intenter une action devant les juridictions compétentes contre un responsable de traitement ou un sous-traitant après saisine de l'APDPVP.

Elle peut, aux fins de défendre ses intérêts, mandater ou se faire représenter par une organisation non gouvernementale ou une association œuvrant dans le domaine de la protection des données.

Sous-section 4 : Des sanctions pénales

Article 212 : Les infractions pénales résultants de la violation des dispositions de la présente loi, sont réprimées conformément aux dispositions du code pénal.

Article 213 : Est puni d'une peine d'emprisonnement de six mois à un an et d'une amende de un millions à dix millions de francs CFA, le fait d'entraver l'action de l'APDPVP soit en :

-s'opposant à l'exercice des missions confiées à ses membres ou aux agents habilités ;
-refusant de communiquer à ses membres ou aux agents habilités, les renseignements et documents utiles à leur mission, ou en dissimulant lesdits documents ou renseignements, ou en les faisant disparaître ;
-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.

En cas de récidive, les peines prévues à l'alinéa précédent sont portées au double.

Article 214 : En cas de saisine de l'APDPVP, le Procureur de la République informe le Président de l'APDPVP de toutes les poursuites relatives aux infractions au Code Pénal et des suites qui leurs sont données. Il lui indique la date et l'objet de l'audience de jugement par lettre recommandée adressée au moins dix jours avant cette date.

La juridiction d'instruction ou de jugement peut appeler le Président de l'Autorité ou son représentant à déposer ses observations ou à les développer oralement à l'audience.

L'APDPVP est de droit, expert près de la justice gabonaise en matière de données personnelles et de la vie privée.

Chapitre VIII : Des dispositions diverses et finales

Article 215 : Le Président de l'Autorité prend des mesures appropriées, notamment l'adoption par l'Assemblée Plénière d'un manuel des procédures, pour assurer le respect de l'ensemble des obligations résultant de la présente loi.

Article 216 : Les responsables de traitement et leurs sous-traitants sont assujettis à la redevance instituée par la présente loi.

L'assiette, le taux et les modalités de paiement de la redevance sont fixés par la loi des finances, sur proposition de l'Autorité.

Article 217 : Les modalités de répartition du produit de la redevance sont fixées par arrêté conjoint du Ministre chargé des Relations avec les Autorités Administratives Indépendantes et du Ministre chargé de l'Economie et des Finances.

Article 218 : L'Autorité élabore un code de bonne conduite en fonction de la spécificité des secteurs relevant de sa compétence.

Article 219 : Les responsables de traitement sont tenus de se conformer dès publication de la présente loi.

Article 220 : Des textes réglementaires déterminent, en tant que de besoin, les dispositions de toute nature nécessaires à l'application de la présente loi.

Article 221 : La présente loi, qui abroge toutes dispositions antérieures contraires, notamment certaines dispositions de la loi n°001/2011 du 25 septembre 2011 relative à la Protection des Données à Caractère Personnel, sera enregistrée, publiée au Journal Officiel et exécutée comme loi de la République.

Fait à Libreville, le 12 juillet 2023

Le Président de la République,
Chef de l'Etat

Ali BONGO ONDIMBA

Le Premier Ministre, Chef du Gouvernement
Alain-Claude BILIE-BY-NZE

Le Ministre d'Etat, Ministre des Relations avec les Institutions Constitutionnelles et les Autorités Administratives Indépendantes
Denise MEKAM'NE EDZIDZIE TATY

Le Ministre d'Etat, Ministre de l'Intérieur
Lambert Noël MATHA

Le Ministre de la Défense Nationale
Félicité ONGOUORI NGOUBILI

Le Ministre de la Santé et des Affaires Sociales
Guy Patrick OBIANG NDONG

Le Ministre de l'Economie Numérique
Jean Pierre DOUKAGA KASSA

Le Ministre du Budget et des Comptes Publics
Edith EKIRI MOUNOMBI épouse OYOUOMI

Le Ministre de la Communication
Rodrigue MBOUMBA BISSAWOU

Loi n°026/2023 du 12 juillet 2023 autorisant l'Etat Gabonais à contracter un emprunt d'un montant équivalent à cinquante millions (50.000.000) de dollars US auprès de la Banque Arabe pour le Développement Economique en Afrique (BADEA)

L'Assemblée Nationale et le Sénat ont délibéré et adopté ;
Le Président de la République, Chef de l'Etat, promulgue la loi dont la teneur suit :

Article 1er : L'Etat Gabonais est autorisé à contracter un emprunt d'un montant de cinquante millions (50.000.000) de dollars US, équivalent à vingt-neuf milliards huit cent quatre-vingt-douze millions (29 892 000 000) de Francs CFA auprès de la Banque Arabe pour le Développement Economique en Afrique, en abrégé BADEA.

Article 2 : Le produit de l'emprunt spécifié et autorisé à l'article 1er ci-dessus est destiné au financement d'un programme d'appui budgétaire qui sera affecté au secteur de la santé et au développement des infrastructures.

Article 3 : Le Ministre de l'Economie et de la Relance est habilité à conclure et à signer, au nom et pour le compte de l'Etat Gabonais, la convention de prêt ainsi que les autres documents y relatifs.

Article 4 : La présente loi sera enregistrée, publiée au Journal Officiel et exécutée comme loi de la République.

Fait à Libreville, le 12 juillet 2023

Le Président de la République,
Chef d'Etat

Ali BONGO ONDIMBA

Le Premier Ministre, Chef du Gouvernement
Alain-Claude BILIE-BY-NZE

Le Ministre de l'Economie et de la Relance
Nicole Jeanine Lydie ROBOTY épouse MBOU

Le Ministre de la Santé et des Affaires Sociales
Guy Patrick OBIANG NDONG

Loi n°027/2023 du 12 juillet 2023 portant règlementation de la cybersécurité et de la lutte contre la cybercriminalité en République Gabonaise

L'Assemblée Nationale et le Sénat ont délibéré et adopté,
Le Président de la République, Chef de l'Etat,
Promulgue la loi dont la teneur suit :

Article 1er : La présente loi, prise en application des dispositions de l'article 47 de la Constitution, porte réglementation de la cybersécurité et de la lutte contre la cybercriminalité en République Gabonaise.

Titre premier : Des dispositions générales

Chapitre Ier : De l'objet et du champ d'application

Article 2 : La présente loi a pour objet d'adapter les dispositifs de sécurité de la République Gabonaise aux enjeux de la société de l'information.

A ce titre, elle vise notamment à :

-organiser la sécurité des systèmes d'information et instaurer une confiance des citoyens, des entreprises et des pouvoirs publics à l'égard de l'usage des technologies de l'information et de la communication ;
-définir et réprimer toute infraction commise au moyen des technologies de l'information et de la communication ;
-fixer les règles et les dispositions générales de sécurité applicables aux réseaux de communications électroniques et aux systèmes d'information de l'Etat et ses démembrements ;
-fixer les règles et dispositions générales de sécurité applicables aux prestataires de services de la société de l'information et aux opérateurs d'infrastructures critiques ;
-protéger les droits fondamentaux des personnes physiques, notamment le droit à la dignité humaine, à l'honneur et au respect de la vie privée, ainsi que les intérêts légitimes des personnes morales ;
-protéger les opérateurs d'infrastructures critiques ;
-promouvoir l'utilisation des technologies de sécurité de l'information en tant que moyens de protection des droits de propriété intellectuelle ;
-assurer l'équilibre entre les intérêts du secteur public et ceux du secteur privé.

Article 3 : Les dispositions de la présente loi s'appliquent à tout usage des technologies de l'information et de la communication produisant ses effets au Gabon.

Est réputé produire ses effets au Gabon, tout usage des technologies de l'information et de la communication, sur le territoire de la République Gabonaise ou non par une personne physique ou morale de nationalité gabonaise ou étrangère contre :

-des droits ou intérêts de la République Gabonaise ou des intérêts s'y rapportant indirectement ;
-des droits ou intérêts des personnes physiques ou morales de nationalité gabonaise ;
-des personnes physiques ou morales de nationalité étrangère domiciliées ou dont les intérêts en République Gabonaise sont impactés.

Article 4 : Les dispositions de la présente loi ne s'appliquent pas aux :

-dispositifs spécifiques utilisés en matière de défense et de sécurité nationale ;
-moyens de cryptologie utilisés par les missions diplomatiques et consulaires visées par la Convention de Vienne sur les relations diplomatiques ainsi que ceux relatifs à la sécurité de l'Etat.

Chapitre II : Des définitions

Article 5 : Au sens de la présente loi, on entend par :

-**accès dérobé** : mécanisme permettant de prévoir un accès tenu secret vis-à-vis de l'utilisateur légitime aux données contenues dans un logiciel ou sur un matériel ;
-**accès illicite** : accès intentionnel, sans en avoir le droit, à l'ensemble ou à une partie d'un réseau de communications électroniques, d'un système d'information ou d'un équipement terminal ;
-**activité de cryptologie** : toute activité ayant pour but la production, l'utilisation, l'importation, l'exportation ou la commercialisation des moyens de cryptologie ;
-**agrément** : reconnaissance formelle que le produit ou le système évalué peut protéger jusqu'à un niveau spécifié par un organisme agréé ;
-**algorithme** : suite d'opérations mathématiques élémentaires à appliquer à des données pour aboutir à un résultat désiré ;
-**algorithme cryptologique** : procédé permettant, avec l'aide d'une clé, de chiffrer et de déchiffrer des messages ou des documents ;
-**algorithme asymétrique** : algorithme de chiffrement utilisant une clé publique pour chiffrer et une clé privée différente de cette dernière pour déchiffrer les messages ;
-**algorithme symétrique** : algorithme de déchiffrement utilisant une même clé pour chiffrer et déchiffrer les messages ;
-**attaque active** : acte modifiant ou altérant les ressources ciblées par l'attaque tel que l'atteinte à l'intégrité, à la disponibilité et à la confidentialité des données ;
-**attaque passive** : acte n'altérant pas sa cible tel que l'écoute passive ou l'atteinte à la confidentialité ;
-**atteinte à l'intégrité** : fait de provoquer intentionnellement une perturbation grave ou une interruption de fonctionnement d'un système d'information, d'un réseau de communications électroniques ou d'un équipement terminal, en introduisant, transmettant, endommageant, effaçant, détériorant, modifiant, supprimant ou rendant inaccessibles les données ;
-**audit de sécurité** : examen méthodique des composantes et des acteurs de la sécurité, de la politique, des mesures, des solutions, des procédures et des moyens mis en œuvre par une organisation, pour sécuriser son environnement ;
-**authentification** : critère de sécurité défini par un processus mis en œuvre notamment pour vérifier l'identité d'une personne physique ou morale et s'assurer que l'identité fournie correspond à l'identité de cette personne préalablement enregistrée ;
-**autorité administrative** : toute autorité administrative investie des prérogatives administratives dans le domaine du numérique ;
-**autorité ministérielle compétente** : autorité ministérielle en charge du secteur de l'économie numérique ou toute autre autorité ministérielle ;
-**bi-clé** : couple clé publique et clé privée utilisé dans des algorithmes de cryptographie asymétrique ;
-**chiffrement** : toute technique, tout procédé grâce auquel sont transformées à l'aide d'une convention secrète appelée clé, des données numériques, des informations claires en informations inintelligibles par des tiers n'ayant pas connaissance de la clé ;
-**chiffrement par bloc** : chiffrement opérant sur des blocs d'informations claires et sur des informations chiffrées ;
-**chiffrer** : action visant à assurer la confidentialité d'une information, à l'aide de codes secrets, pour la rendre inintelligible à des tiers, en utilisant des mécanismes offerts en cryptographie ;
-**clé** : valeur mathématique, mot ou phrase qui permet, grâce à l'algorithme de chiffrement, de chiffrer ou de déchiffrer un message dans un système de chiffrement ;
-**clé de chiffrement** : série de symboles commandant les opérations de chiffrement et de déchiffrement ;
-**clé privée** : clé utilisée dans les mécanismes de chiffrement asymétrique ou chiffrement à clé publique, appartenant à une entité et devant être secrète ;
-**clé publique** : clé servant au chiffrement d'un message dans un système asymétrique et donc librement diffusé ;
-**clé sécrète** : clé connue de l'émetteur et du destinataire servant de chiffrement et de déchiffrement des messages et utilisant le mécanisme de chiffrement symétrique ;
-**code source** : ensemble des spécifications techniques, sans restriction d'accès ni de mise en œuvre, d'un logiciel ou protocole de communication, d'interconnexion, d'échange ou d'un format de données ;

-**communication électronique** : émission, transmission ou réception, de signes, de signaux, d'écrits, d'images ou de sons par voie électronique ;
-**confidentialité** : maintien du secret des informations et des transactions afin de prévenir la divulgation non autorisée d'informations aux non destinataires permettant la lecture, l'écoute, la copie illicite d'origine intentionnelle ou accidentelle durant leur stockage, traitement ou transfert ;
-**contenu** : ensemble d'informations relatives aux données appartenant à des personnes physiques ou morales, transmises ou reçues à travers les réseaux de communications électroniques et les systèmes d'information ;
-**contenu illicite** : contenu portant atteinte à la dignité humaine, à la vie privée, à l'honneur ou à la sécurité administrative ;
-**convention secrète** : accord de volontés portant sur des 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 ;
-**courrier électronique** : tout message sous forme de texte, de voix, de son ou d'image envoyé par un réseau public ou privé de communication, qui peut être stocké dans le réseau ou dans l'équipement terminal du destinataire jusqu'à ce que ce dernier le récupère ;
-**cryptage** : utilisation de codes ou signaux non usuels permettant la conservation des informations à transmettre en des signaux incompréhensibles par les tiers ;
-**cryptanalyse** : opération qui vise à rétablir une information inimitable en information claire sans connaître la clé de chiffrement qui a été utilisée ;
-**cryptogramme** : message chiffré ou codé ;
-**cryptographie** : ensemble de techniques, application des mathématiques permettant d'écrire l'information, de manière à la rendre inintelligible à ceux ne possédant pas les capacités de la déchiffrer ;
-**cryptologie** : science relative à la protection et à la sécurité des informations notamment pour la confidentialité, l'authentification, l'intégrité et la non répudiation des données transmises ;
-**cybercriminalité** : ensemble des infractions commises au moyen ou sur un réseau de communication électronique ou un système d'information ;
-**cybersécurité** : ensemble de mesures de prévention, de protection et de dissuasion d'ordre technique, organisationnel, juridique, financier, humain, procédural et autres actions permettant d'atteindre les objectifs de sécurité fixés à travers les réseaux de communications électroniques, les systèmes d'information et pour la protection de la vie privée des personnes ;
-**démembrement de l'Etat** : entité étatique décentralisée ;
-**déni de service** : attaque informatique ayant pour effet d'empêcher ou de limiter fortement la capacité d'un système d'information ou du réseau de communications électroniques, à fournir le service attendu ;
-**déni de service distribué** : attaque informatique lancée depuis plusieurs sources ayant pour effet d'empêcher ou de limiter fortement la capacité d'un système d'information ou du réseau de communications électroniques, à fournir le service attendu ;
-**disponibilité** : critère de sécurité permettant que les ressources des réseaux de communications électroniques, des systèmes d'information ou des équipements terminaux soient accessibles et utilisables selon les besoins ;
-**données confidentielles** : informations qui ne doivent être communiquées ou rendues accessibles qu'aux personnes et aux entités autorisées ;
-**données informatiques** : représentation de faits, d'informations ou de notions sous une forme susceptible d'être traitée par un équipement terminal, y compris un programme permettant à ce dernier d'exécuter une fonction ;
-**données de connexion** : ensemble d'informations relatives au processus d'accès dans une communication électronique ;
-**données de trafic** : données ayant trait à une communication électronique indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type du service réseau sous-jacent ;
-**équipement terminal** : tout équipement destiné à être connecté directement ou indirectement à un point de terminaison d'un réseau en vue de la transmission, du traitement ou de la réception d'informations ;
-**fiabilité** : aptitude d'un système d'information ou d'un réseau de communications électronique à fonctionner sans incident pendant un temps suffisamment long ;
-**fournisseur des services de communications électroniques** : personne physique ou morale fournissant à titre principal des prestations de communications électroniques ;
-**gestion des incidents de cybersécurité** : processus de détection, de signalement et d'évaluation des incidents de cybersécurité, ainsi que les mesures d'intervention et de traitement y afférentes ;
-**gravité de l'impact** : appréciation du niveau de gravité d'un incident, pondéré par sa fréquence d'apparition ;
-**infrastructure critique** : installations, ouvrages, systèmes ou partie de ces dispositifs, civils ou militaires, fournissant des biens ou services indispensables au maintien des fonctions vitales de l'État dont l'indisponibilité ou le dysfonctionnement aurait un impact significatif induisant la défaillance de ces fonctions ;
-**incident de cybersécurité** : évènement(s), indésirable(s) ou inattendu(s) lié(s) à la sécurité des systèmes d'information et présentant une forte probabilité de compromettre les activités d'une entité, d'une infrastructure critique ou d'un opérateur d'infrastructure critique ou de menacer la sécurité de leurs systèmes d'information ;
-**intégrité des données** : critère de sécurité définissant l'état d'un réseau de communications électroniques,

d'un système d'information ou d'un équipement terminal qui est demeuré intact et permet de s'assurer que les ressources n'ont pas été altérées ;

-**interception illégale** : accès sans en avoir le droit ou l'autorisation, aux données d'un réseau de communications électroniques, d'un système d'information ou d'un équipement terminal ;

-**interception légale** : accès autorisé aux données d'un réseau de communications électroniques, d'un système d'information ou d'un équipement terminal ;

-**intrusion par intérêt** : accès intentionnel et sans droit dans un réseau de communications électroniques ou dans un système d'information, dans le but soit de nuire soit de tirer un bénéfice économique, financier, industriel, sécuritaire ou de souveraineté ;

-**intrusion par défi intellectuel** : accès intentionnel, sans en avoir le droit ou l'autorisation, dans un réseau de communications électroniques ou dans un système d'information, dans le but de relever un défi intellectuel pouvant contribuer à l'amélioration des performances du système de sécurité de l'organisation ;

-**logiciel trompeur** : logiciel effectuant des opérations sur un équipement terminal d'un utilisateur sans informer préalablement cet utilisateur de la nature exacte des opérations que ce logiciel va effectuer sur son équipement terminal ou sans demander à l'utilisateur s'il consent à ce que le logiciel procède à ces opérations ;

-**logiciel espion** : type particulier de logiciel trompeur collectant les informations personnelles auprès d'un utilisateur du réseau de communications électroniques ;

-**logiciel potentiellement indésirable** : logiciel représentant des caractéristiques d'un logiciel trompeur ou d'un logiciel espion ;

-**matériel raciste et xénophobe** : tout support numérique qui préconise ou encourage la haine, la discrimination ou la violence, contre une personne ou un groupe de personnes, en raison de la race, de la couleur, de la religion, de l'ascendance ou de l'origine nationale ou ethnique ;

-**moyens de cryptologie** : ensemble d'outils scientifiques et techniques permettant de chiffrer ou de déchiffrer ;

-**non répudiation** : critère de sécurité assurant la disponibilité de preuves qui peuvent être opposées à un tiers et utilisées pour prouver la traçabilité d'une communication électronique qui a eu lieu ;

-**opérateur** : toute personne morale ou physique, privée ou publique, exploitant une infrastructure ou fournissant un service à destination du public ;

-**opérateur d'infrastructures critiques** : opérateur exploitant une infrastructure ou fournissant un service critique ;

-**politique de sécurité** : référentiel de sécurité établi par une organisation, reflétant sa stratégie de sécurité et spécifiant les moyens de la réaliser ;

-**pornographie enfantine** : toute donnée quelle qu'en soit la nature ou la forme ou le support représentant : un mineur se livrant à un comportement sexuellement explicite ;

-des images réalistes représentant un mineur se livrant à un comportement sexuellement explicite.

-**prestation de cryptographie** : opération visant à la mise en œuvre, pour le compte d'autrui ou de soi, de moyens de cryptographie ;

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

-**preuve numérique** : indices digitaux sous forme d'informations qui se concrétisent au travers des données numériques ;

-**prospection directe** : tout envoi de tout message destiné à promouvoir, directement ou indirectement, des biens, des services ou l'image d'une personne vendant des biens ou fournissant des services ;

-**réseau de communications électroniques** : système de transmission permettant l'acheminement de signaux par câble, par voie hertzienne, par moyen optique ou par d'autres moyens électromagnétiques ;

-**sécurité** : situation dans laquelle quelqu'un, quelque chose n'est exposé à aucun danger. Mécanisme destiné à prévenir un événement dommageable, ou à limiter les effets ;

-**service critique** : service à la fois publics et privés, indispensables au maintien des fonctions vitales de l'Etat et de la société, de la santé, de la sûreté, de la sécurité et du bien-être économique ou social des citoyens, et dont l'arrêt ou la destruction aurait un impact significatif du fait de la défaillance de ces fonctions ;

-**système de détection** : système permettant de détecter les incidents qui pourraient conduire aux violations de la politique de sécurité et permettant de diagnostiquer des intrusions potentielles ;

-**système d'information** : ensemble organisé de ressources permettant de collecter, regrouper, classifier, traiter et diffuser l'information ;

-**système informatique** : tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure un traitement automatisé de données ;

-**vulnérabilité** : défaut ou insuffisance de sécurité, connu ou inconnu, dans l'architecture d'un réseau de communications électroniques ou dans la conception d'un système d'information se traduisant par une violation de la politique de sécurité.

Article 6 : La présente loi intègre, en tant que de besoin, les autres définitions contenues dans tout autre texte en vigueur, en rapport avec la cybersécurité ou la cybercriminalité.

Les termes et références non définis dans la présente loi conservent leurs définitions ou significations données par les instruments juridiques internationaux ratifiés par l'Etat Gabonais.

Titre II : Du cadre institutionnel de la cybersécurité et de la lutte contre la cybercriminalité

Article 7 : Le cadre institutionnel comprend notamment :

-le Ministère en charge de l'Economie Numérique ;
-le Ministère en charge de la Justice ;
-le Ministère en charge de la Défense Nationale ;
-le Ministère en charge de la Sécurité ;
-le Ministère en charge de l'Economie ;
-le Ministère en charge du Budget et des Comptes Publics ;
-les institutions et organismes de support ou d'appui.

Les attributions détaillées des administrations, institutions et organismes cités ci-dessus sont fixées par les dispositions des textes législatifs et réglementaires.

Titre III : De la cybersécurité

Article 8 : Les dispositions et mesures relevant de la cybersécurité sont définies et mises en œuvre sous l'autorité du Gouvernement.

Le Gouvernement définit une stratégie nationale en matière de cybersécurité. Cette stratégie est adoptée par décret.

Chapitre Ier : De la protection des infrastructures et services critiques

Article 9 : Un décret pris en Conseil des Ministres, sur proposition conjointe des Ministres chargés de la Défense Nationale et de la Sécurité, adopte des normes et procédures relatives aux politiques de défense, de sécurité des infrastructures et services critiques et des plans de rétablissement définis par l'autorité administrative compétente en matière de sécurité des systèmes d'information déterminée par les textes en vigueur.

Article 10 : Un décret pris en conseil des Ministres, sur proposition conjointe des Ministres chargés de la Défense nationale et de la Sécurité, adopte les critères de classification des opérateurs d'infrastructures et services critiques définis par l'autorité administrative compétente.

Article 11 : Chaque département ministériel identifie les infrastructures et services critiques relevant de son secteur, notamment dans les domaines régalien, humain, économique et technologique, après avis notamment, de l'autorité administrative compétente.

La liste de ces secteurs et infrastructures critiques fait l'objet d'un décret de classification notifié à l'opérateur de l'infrastructure critique dans les mêmes formes.

Article 12 : L'opérateur d'une infrastructure critique établit, sur la base des résultats d'une analyse des risques, la liste des systèmes d'information sensibles et la transmet avec les mises à jour de celle-ci à l'autorité administrative compétente.

L'autorité administrative compétente peut faire des observations à l'opérateur de l'infrastructure critique, sur la liste des systèmes d'information sensibles qui lui a été transmise.

Dans ce cas, l'opérateur de l'infrastructure critique est tenu de modifier sa liste conformément à ces observations et transmet la liste modifiée à l'autorité administrative compétente, dans un délai fixé par un texte réglementaire.

La liste des systèmes d'information sensibles est couverte par le degré de classification correspondant.

Article 13 : L'opérateur d'une infrastructure critique est tenu de prendre toutes dispositions utiles en vue d'organiser et d'assurer la sécurité de cette infrastructure, dans les conditions et selon les modalités fixées par voie réglementaire.

Un arrêté conjoint des Ministres chargés de la Défense, de la Sécurité et de l'Economie Numérique, définit un cadre de coopération entre les opérateurs d'infrastructures critiques sous la coordination de l'autorité administrative compétente.

Le cadre de coopération visé au précédent alinéa garantit un échange permanent d'informations entre les acteurs, notamment sur les menaces et vulnérabilités et la mise en place de procédures permettant de prévenir et détecter les incidents de cybersécurité et d'y répondre efficacement.

Article 14 : Les opérateurs dont un ou plusieurs établissements, installations et ouvrages, désignés en application de l'article 12 ci-dessus, réalisent pour chacun de ces établissements, installations ou ouvrages des mesures de protection particulières.

Le plan d'exécution de ces mesures, élaboré par l'opérateur, est soumis à l'approbation de l'autorité administrative compétente.

En cas de non-approbation du plan ou de désaccord, la décision est prise par l'autorité administrative compétente.

Article 15 : Les mesures de protection visées aux articles 13 et 14 ci-dessus comportent notamment des dispositifs de surveillance, d'alerte et de protection matérielle ayant pour effet de garantir l'opérationnalité permanente de l'infrastructure.

Article 16 : Le plan des mesures de protection est élaboré par l'opérateur et soumis à l'approbation de l'autorité administrative compétente.

La réalisation effective de ces mesures fait l'objet d'une certification de sécurité.

Article 17 : En cas d'approbation du plan de protection, l'autorité administrative compétente impartit à l'opérateur un délai d'exécution.

L'inobservation de ce délai expose l'opérateur défaillant à une amende dont le montant est fixé en fonction de l'importance du dommage résultant de l'impact causé ou susceptible d'être causé.

Les modalités d'application de cette amende sont fixées par la loi de finances.

Une copie de ce plan est transmise à chaque autorité ministérielle compétente.

Article 18 : Par exception aux dispositions de l'article 17 ci-dessus, les entreprises nationales ou faisant appel au concours financier de l'Etat sont mises en demeure en cas d'inexécution dans le délai fixé pour la réalisation du plan de protection.

Les mises en demeure sont communiquées aux autorités de tutelle de ces entreprises.

Chapitre II : De la protection des réseaux de communications électroniques

Article 19 : Les opérateurs des réseaux de communications électroniques et les fournisseurs de services de communications électroniques doivent prendre toutes les mesures techniques et administratives nécessaires pour garantir la sécurité des services offerts.

A ce titre, ils sont notamment tenus d'informer les usagers :

-du danger encouru en cas d'utilisation de leurs réseaux ;
-des risques particuliers de violation de la sécurité ;
-de l'existence de moyens techniques permettant d'assurer la sécurité de leurs communications.

En outre, les opérateurs des réseaux sont tenus de mettre en place un dispositif d'enregistrement pour recueillir les réclamations et les signalements des usagers.

Les modalités d'application du présent article sont fixées par voie réglementaire.

Article 20 : Les opérateurs de réseaux et les fournisseurs de services de communications électroniques ont l'obligation de conserver les données de connexion et de trafic pendant une période de dix ans sur le territoire national à compter de la date de leur enregistrement. Au terme de ce délai, les opérateurs et les fournisseurs doivent transmettre à l'autorité le procès-verbal de la suppression desdites données de connexion et de trafic.

Les opérateurs de réseaux et les fournisseurs de services de communications électroniques installent des mécanismes de surveillance de trafic des données de leurs réseaux. Ces données sont accessibles lors des investigations judiciaires.

Article 21 : La responsabilité des opérateurs de réseaux et celle des fournisseurs de services de communications électroniques n'est pas engagée si l'utilisation des données prévue à l'alinéa 2 ci-dessus porte atteinte aux libertés individuelles des usagers.

Article 22 : Les opérateurs de réseaux de communications électroniques installés sur le territoire national sont tenus de disposer d'un centre de gestion opérationnelle de leurs infrastructures et de leurs données sur le territoire national.

Chapitre III : De la protection des systèmes d'information

Section 1 : Dispositions spécifiques à l'Etat et ses démembrements

Article 23 : Les données, les infrastructures numériques et systèmes d'information de l'Etat et ses démembrements doivent être classifiés selon leur niveau de sensibilité en termes de confidentialité, d'intégrité et de disponibilité. Les mesures de protection de ces actifs informationnels doivent être proportionnées au niveau de classification attribué.

Chaque administration ou démembrement de l'Etat doit arrêter des procédures d'habilitation des personnes pouvant accéder aux informations classifiées et des conditions d'échange, de conservation ou de transport de ces informations. Le référentiel de classification des actifs informationnels et des systèmes d'information est fixé par voie réglementaire.

Article 24 : Chaque administration ou démembrement de l'Etat met en place une équipe chargée d'appliquer la politique de sécurité du système d'information en collaboration avec l'autorité administrative compétente en matière de cybersécurité conformément aux dispositions des textes en vigueur.

Chaque administration désigne un responsable au sein de cette équipe. Ce dernier est l'interlocuteur de l'autorité administrative compétente en matière de cybersécurité et doit jouir de l'indépendance requise dans l'exercice de sa mission.

Article 25 : Chaque administration ou démembrement de l'Etat doit, dès qu'il a connaissance d'un incident de cybersécurité, le déclarer à l'autorité administrative compétente.

Un décret d'application précise les conditions d'application du présent article.

Article 26 : L'externalisation à un prestataire de service d'un système d'information sensible au sens de l'article 23 de la présente loi est subordonnée à un avis motivé de l'autorité administrative compétente, ce dernier est tenu de respecter au maximum, les normes et référentiels techniques relatifs à la sécurité des systèmes d'information édictés par l'autorité administrative compétente.

Sous réserve d'une dérogation écrite accordée par l'autorité administrative compétente, l'externalisation d'un système d'information sensible doit faire l'objet d'un contrat régi par le droit gabonais, contenant obligatoirement des engagements de protection de l'information, d'auditabilité et de réversibilité des données.

Article 27 : Les données jugées confidentielles ou sensibles au sens de l'article 22 de la présente loi, doivent être exclusivement hébergées sur le territoire national, sauf dérogation écrite de l'autorité administrative compétente.

Section 2 : Des dispositions communes

Article 28 : Les exploitants des systèmes d'information prennent toutes les mesures techniques et administratives afin de garantir la sécurité des services offerts. A ce titre, ils se dotent de systèmes normalisés leur permettant d'identifier, d'évaluer, de traiter et de gérer en continu les risques liés à la sécurité des systèmes d'information.

Les exploitants des systèmes d'information mettent en place des mécanismes techniques permettant de faire face aux atteintes préjudiciables à la disponibilité permanente des systèmes, à leur intégrité, à leur authentification, à leur non-répudiation par des utilisateurs tiers, à la confidentialité des données et à la sécurité physique.

Les mécanismes prévus à l'alinéa 2 du présent article, font l'objet d'un visa de conformité à la politique administrative de cybersécurité de la part de l'autorité administrative compétente.

Les systèmes d'information font l'objet de protection contre d'éventuels rayonnements et d'intrusions qui peuvent compromettre l'intégrité des données transmises et contre toute autre attaque.

Article 29 : Les personnes dont l'activité est d'offrir un accès à des systèmes d'information sont notamment tenues d'informer les usagers :

-du danger encouru dans l'utilisation des systèmes d'information non sécurisés ;
-de la nécessité d'installer des dispositifs de contrôle parental ;
-des risques particuliers de violation de sécurité ;
-de l'existence de moyens techniques permettant de restreindre l'accès à certains services et de leur proposer au moins l'un de ces moyens.

Article 30 : Les exploitants des systèmes d'information informent les utilisateurs de l'interdiction faite d'utiliser les réseaux de communications électroniques pour diffuser des contenus illicites ou tout autre acte qui peut entamer la sécurité des réseaux ou des systèmes d'information.

L'interdiction porte également sur la conception de logiciel trompeur, espion, potentiellement indésirable ou de tout autre outil conduisant à un comportement frauduleux.

Article 31 : Les exploitants des systèmes d'information ont l'obligation de conserver les données de connexion et de trafic de leurs systèmes d'information pendant une période de dix ans.

Article 32 : Les exploitants des systèmes d'information sont tenus d'installer des mécanismes de surveillance et de contrôle d'accès aux données de leurs systèmes d'information. Les données conservées sont accessibles lors des investigations judiciaires.

Les installations des exploitants des systèmes d'information peuvent faire l'objet de perquisition ou de saisie sur ordre d'une autorité judiciaire dans les conditions prévues par les lois en vigueur.

Les dispositions du présent article sont sans préjudice notamment, du respect des textes en vigueur, notamment la loi relative à la protection des données à caractère personnel.

Article 33 : Les exploitants des systèmes d'information évaluent, révisent leurs systèmes de sécurité et introduisent en cas de nécessité les modifications appropriées dans leurs pratiques, mesures et techniques de sécurité en fonction de l'évolution des technologies.

Les exploitants des systèmes d'information et leurs utilisateurs peuvent coopérer pour l'élaboration et la mise en œuvre des pratiques, mesures et techniques de sécurité de leurs systèmes.

Article 34 : Les réseaux de communications électroniques et les systèmes d'information sont soumis à un régime d'audit de sécurité obligatoire et périodique de leurs systèmes de sécurité, selon les modalités fixées par voie réglementaire.

Article 35 : Les dispositions de la présente section s'appliquent aux opérateurs d'infrastructures critiques,

sous réserve de l'application de mesures de sécurité plus contraignantes, selon les modalités fixées par voie réglementaire.

Chapitre IV : De la protection des contenus

Article 36 : Tout opérateur est tenu d'héberger une copie de ses données sur le territoire national, dans les conditions et selon les modalités fixées par voie réglementaire.

Article 37 : Les opérateurs et exploitants des réseaux de communications électroniques et des systèmes d'information assurent la confidentialité des communications acheminées à travers les réseaux de communications électroniques et les systèmes d'information y compris les données relatives au trafic.

Article 38 : Il est interdit à toute personne physique ou morale, équipements informatiques ou intelligence artificielle d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic y afférent, ou de les soumettre à tout autre moyen d'interception ou de surveillance, sans le consentement des utilisateurs concernés, sauf lorsque cette personne y est légalement autorisée.

Toutefois, le stockage technique préalable à l'acheminement de toute communication est autorisé aux opérateurs et exploitants des réseaux de communications électroniques, sans préjudice du principe de confidentialité.

Article 39 : L'enregistrement des communications et des données de trafic y afférent, effectué dans le cadre professionnel en vue de fournir la preuve numérique d'une communication électronique, est autorisé dans les conditions fixées par la présente loi.

Article 40 : Les prestataires ou fournisseurs des services de communications électroniques, sont tenus d'informer leurs abonnés de l'existence de moyens techniques permettant de restreindre l'accès à certains services, de les sélectionner ou de leur proposer au moins un de ces moyens.

Article 41 : La confidentialité des communications acheminées à travers les réseaux de communications électroniques et les systèmes d'information, y compris les données relatives au trafic, est assurée par les opérateurs et exploitants des réseaux de communications électroniques et des systèmes d'information.

Article 42 : Les fournisseurs de contenus des réseaux de communications électroniques et systèmes d'information sont tenus d'assurer la disponibilité des contenus, ainsi que celle des données stockées dans leurs installations, selon les modalités fixées par voie réglementaire.

Ils ont l'obligation de mettre en place des filtres pour faire face aux atteintes préjudiciables aux données personnelles et à la vie privée des utilisateurs.

Article 43 : Les fournisseurs de contenus des réseaux de communications électroniques et systèmes d'information, sont tenus de conserver les contenus ainsi que les données stockées dans leurs installations pendant une durée de dix ans.

Les fournisseurs de contenus des réseaux de communications électroniques et systèmes d'information, ont l'obligation de mettre en place des filtres pour faire face aux atteintes préjudiciables aux données personnelles et à la vie privée des utilisateurs.

Article 44 : L'utilisation des réseaux de communications électroniques et des systèmes d'information aux fins de stocker les informations ou d'y accéder à des informations stockées dans un équipement terminal d'une personne physique ou morale, ne peut se faire qu'avec le consentement préalable de la personne concernée ou d'un tiers légalement autorisé.

Article 45 : L'émission des messages électroniques à des fins de prospection en dissimulant l'identité de l'émetteur au nom duquel la communication est faite, ou sans indiquer une adresse valide à laquelle le destinataire peut transmettre une demande visant à obtenir l'arrêt de ces informations est interdite.

L'émission des messages électroniques utilisant frauduleusement l'identité d'autrui est interdite.

Article 46 : Les personnels des opérateurs des réseaux de communications électroniques ou des fournisseurs de services de communications électroniques sont astreints au secret professionnel.

Chapitre V : De la cryptologie

Article 47 : Les modalités d'utilisation de la taille de certaines clés sont fixées par voie réglementaire.

Le prestataire ou la personne procédant à la fourniture d'un service de cryptologie tient à la disposition de l'autorité administrative compétente une description des caractéristiques techniques de ce moyen de cryptologie, ainsi que le code source des logiciels utilisés.

La cryptologie est un domaine de souveraineté de l'Etat.

Les prestataires de services de cryptologie sont assujettis au secret professionnel.

Un texte réglementaire précise les modalités d'application du présent article.

Titre IV : De la cybercriminalité

Article 48 : Les dispositions du présent titre prévalent sur celles des autres textes en vigueur en matière de prévention et de répression de la cybercriminalité, à l'exception toutefois de celles des textes sous régionaux et internationaux ayant force exécutoire au Gabon.

Chapitre I^er^ : Des infractions et des sanctions

Article 49 : Quiconque accède frauduleusement à tout ou partie d'un système informatique est puni d'un emprisonnement de dix ans et d'une amende de 100.000.000 de francs au plus ou de l'une de ces deux peines.

L'accès frauduleux visé à l'alinéa 1^er^ ci-dessus s'entend également du dépassement d'un accès autorisé.

Article 50 : Quiconque se maintient frauduleusement dans tout ou partie d'un système informatique est puni d'un emprisonnement de cinq ans et d'une amende de 50.000.000 de francs au plus ou de l'une de ces deux peines.

Article 51 : Quiconque entrave le fonctionnement d'un système informatique est puni d'un emprisonnement de cinq ans et d'une amende de 50.000.000 de francs au plus ou de l'une de ces deux peines.

Article 52 : Quiconque introduit frauduleusement des données informatiques dans un système informatique est puni d'un emprisonnement de dix ans et d'une amende de 100.000.000 de francs au plus ou de l'une de ces deux peines.

Article 53 : Quiconque intercepte frauduleusement par des moyens techniques des données informatiques lors de leur transmission non publique à destination, en provenance ou à l'intérieur d'un système informatique, y compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données informatiques, est puni d'un emprisonnement de dix ans et d'une amende de 100.000.000 de francs au plus ou de l'une de ces deux peines.

Article 54 : Quiconque introduit, altère, supprime, extrait frauduleusement des données informatiques est puni d'un emprisonnement de dix ans et d'une amende de 100.000.000 de francs au plus ou de l'une de ces deux peines.

Article 55 : Quiconque fait intentionnellement, usage des données obtenues dans les conditions énoncées par les dispositions des articles ci-dessus est puni d'un emprisonnement de dix ans et d'une amende de 100.000.000 de francs au plus ou de l'une de ces deux peines.

Article 56 : Quiconque importe, détient, offre, cède, vend ou met à disposition illégalement, sous quelque forme que ce soit, un programme informatique, un mot de passe, un code d'accès ou toutes données informatiques similaires conçus ou spécialement adaptés, pour permettre d'accéder, à un réseau de communications électroniques ou un système d'information est puni d'un emprisonnement de dix ans et d'une amende de 100.000.000 de francs au plus ou de l'une de ces deux peines.

Est également puni des peines prévues à l'alinéa 1^er^ ci-dessus, quiconque intentionnellement provoque une perturbation grave ou une interruption d'un réseau de communications électroniques ou d'un système d'information.

Article 57 : Tout prestataire de services de cryptologie qui ne satisfait pas à l'obligation de communiquer la description des caractéristiques techniques du moyen de cryptologie dans les conditions prévues par la présente loi, est puni d'un emprisonnement de deux ans et d'une amende de 2.000.000 de francs au plus ou de l'une de ces deux peines.

Article 58 : Quiconque fournit ou importe un moyen de cryptologie n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité sans satisfaire à l'obligation de déclaration préalable, est punie d'un emprisonnement de cinq ans et d'une amende de 5.000.000 de francs au plus ou de l'une de ces deux peines.

Article 59 : Quiconque exporte un moyen de cryptologie n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité sans avoir obtenu préalablement l'autorisation, est puni d'un emprisonnement de cinq ans et d'une amende de 20.000.000 de francs au plus ou de l'une de ces deux peines.

Article 60 : Quiconque fournit des prestations de cryptologie sans avoir obtenu préalablement l'agrément requis est puni d'un emprisonnement de cinq ans et d'une amende de 20.000.000 de francs au plus ou de l'une de ces deux peines.

Article 61 : Quiconque met à la disposition d'autrui un moyen de cryptologie ayant fait l'objet d'une interdiction d'utilisation et de mise en circulation, est puni d'un emprisonnement de cinq ans et d'une amende de 20.000.000 de francs au plus ou de l'une de ces deux peines.

Article 62 : Quiconque fait obstacle à l'exercice de la mission de contrôle est puni d'un emprisonnement d'un an à cinq ans et d'une amende de 20.000.000 de francs au plus ou de l'une de ces deux peines.

Article 63 : Quiconque met en place un accès dérobé à des données ou à un système d'information sans l'autorisation de l'utilisateur légitime, est puni d'un emprisonnement de cinq ans et d'une amende de 30.000.000 de francs au plus ou de l'une de ces deux peines.

Article 64 : Quiconque produit, enregistre, met à disposition, transmet, importe ou exporte de la pornographie enfantine par le biais d'un système informatique est puni d'un emprisonnement de dix ans et d'une amende de 100.000.000 de francs au plus ou de l'une de ces deux peines.

Article 65 : Quiconque se procure de la pornographie enfantine par le biais d'un système informatique, est puni d'un emprisonnement de cinq ans et d'une amende de 20.000.000 de francs au plus ou de l'une de ces deux peines.

Article 66 : Quiconque détient de la pornographie enfantine dans un système informatique, est puni d'un emprisonnement de cinq ans et d'une amende de 20.000.000 de francs au plus ou de l'une de ces deux peines.

Article 67 : Quiconque facilite l'accès ou diffuse à des mineurs des images, des documents, du son ou une représentation à caractère pornographique, est puni d'un emprisonnement de dix ans et d'une amende de 10.000.000 de francs au plus ou de l'une de ces deux peines.

Article 68 : Quiconque propose, par voie électronique, une rencontre à un enfant mineur, dans le but de commettre à son encontre une des infractions prévues par les articles 48 à 51 ci-dessus, est puni d'un emprisonnement de deux ans et d'une amende de 20.000.000 de francs au plus ou de l'une de ces deux peines.

Article 69 : Quiconque propose ou met à disposition par voie électronique tout produit ou substance illicite, est puni d'un emprisonnement de cinq ans et d'une amende de 10.000.000 de francs au plus ou de l'une de ces deux peines.

Article 70 : Quiconque crée, télécharge, diffuse ou met à disposition sous quelque forme que ce soit, par voie électronique des contenus racistes ou xénophobes, est puni d'un emprisonnement de cinq à dix ans et d'une amende de cinq à 10.000.000 de francs au plus ou de l'une de ces deux peines.

Article 71 : Quiconque profère une menace ou une insulte par voie électronique, envers une personne en raison de son appartenance à un groupe, une race, une couleur, une ascendance, une religion ou une origine, est puni d'un emprisonnement de dix ans et d'une amende de 30.000.000 de francs au plus ou de l'une de ces deux peines.

Article 72 : Est puni d'un emprisonnement de cinq ans et d'une amende 10.000.000 de francs au plus ou de l'une de ces deux peines, quiconque aura volontairement :

-utilisé un système informatique protégé pour relayer ou retransmettre des courriers électroniques multiples dans l'intention de tromper ou d'induire en erreur, quant à l'origine de ces messages les destinataires ou tout prestataire de services de courriers électroniques ou de services internet ;
-falsifié matériellement les informations se trouvant dans les en-têtes de messages électroniques multiples et déclenché leur transmission ;
-déclenché la transmission de courriers électroniques multiples ayant pour origine un logiciel trompeur à partir ou par l'intermédiaire d'un système informatique.

Article 73 : Quiconque utilise frauduleusement l'identité numérique d'un tiers ou une ou plusieurs données permettant de l'identifier, dans l'intention de nuire à autrui, est puni d'un emprisonnement de cinq ans et d'une amende de 10.000.000 de francs au plus ou de l'une de ces deux peines.

Article 74 : Toute atteinte aux biens, aux personnes, aux droits d'autrui commise par voie électronique est punie des peines prévues par les dispositions du Code Pénal.

Article 75 : L'escroquerie, l'abus de confiance, le recel, le chantage, l'extorsion de fonds et le vol commis par voie électronique sont punis des peines prévues par les dispositions du Code Pénal.

Article 76 : Le sursis ne s'applique pas aux infractions prévues par la présente loi.

La tentative et la complicité sont réprimées des mêmes peines que celles prévues pour les infractions auxquelles elles se rapportent.

En cas de récidive, les peines sont portées au double.

Article 77 : Les peines prévues par les dispositions de la présente loi sont portées à vingt-cinq ans de réclusion criminelle et à 500.000.000 de francs d'amende au plus lorsque les infractions ont été commises en bande organisée.

Les peines prévues à l'alinéa ci-dessus s'appliquent également lorsque les infractions en cause portent atteinte aux systèmes d'information de l'Etat et aux infrastructures critiques.

Article 78 : Les auteurs d'atteintes aux dispositions de la présente loi sont passibles des peines complémentaires suivantes :

-la dissolution, lorsque la personne morale s'est détournée de son objet pour commettre les faits incriminés ;
-l'interdiction provisoire ou définitive d'exercer ;
-la fermeture provisoire ou définitive d'un ou de plusieurs des établissements de l'entreprise ;
-l'exclusion provisoire ou définitive de soumissionner ;
-l'interdiction provisoire ou définitive de faire appel public à l'épargne ;
-l'interdiction pour une durée de cinq ans au plus d'émettre des chèques à des tiers ;
-la confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit ;
-l'affichage ou la diffusion de la décision prononcée aux frais de l'auteur des faits.

Chapitre II : De la procédure

Article 79 : La constatation des infractions relevant du champ d'application de la présente loi et des textes pris pour son application est assurée par les Officiers de Police Judiciaire spécialisés habilités par l'autorité administrative compétente et par les Officiers de Police Judiciaire à compétence générale, dans les conditions et selon les modalités prévues par les dispositions des textes en vigueur.

Article 80 : Avant leur entrée en fonctions, les Officiers de Police Judiciaire spécialisés visés à l'article 79 ci-dessus prêtent le serment suivant devant le Tribunal judiciaire territorialement compétent :

« *Je jure d'accomplir ma mission dans le strict respect des textes en vigueur, notamment d'observer les exigences attachées à la présomption d'innocence, à la protection des données personnelles et à la vie privée. Je le jure* ».

Article 81 : Sous l'autorité du Procureur de la République, les Officiers de Police Judiciaire peuvent, dans le cadre de l'exécution de leurs missions, accéder aux moyens de transport, à tout local à usage professionnel, aux domiciles privés, en vue de rechercher, constater les infractions, demander la communication de tous les documents professionnels et en prendre copie, recueillir, sur convocation ou sur place, les renseignements et justificatifs.

Article 82 : Les perquisitions en matière de cybercriminalité sont susceptibles de porter sur les objets, documents et données qui peuvent être des supports physiques ou des copies réalisées en présence des personnes qui assistent à la perquisition.

Lorsqu'une copie des données saisies a été faite, celle-ci peut être détruite sur instruction du Procureur de la République pour des raisons de sécurité. Dans ce cas, seuls seront gardés sous scellé par l'Officier de Police Judiciaire, les objets, documents et données utilisés pour la manifestation de la vérité.

Les personnes présentes lors de la perquisition peuvent être réquisitionnées en vue de fournir les renseignements sur les objets, documents et données saisis.

Article 83 : Les perquisitions et les saisies sont effectuées conformément aux dispositions des textes en vigueur.

Article 84 : Lorsqu'il apparaît que les données saisies ou obtenues au cours de l'enquête ou de l'instruction ont fait l'objet d'opérations de transformation empêchant d'accéder en clair ou sont de nature à compromettre les informations qu'elles contiennent, le Procureur de la République, le Juge d'Instruction ou la juridiction de jugement peuvent réquisitionner toute personne physique ou morale qualifiée, en vue d'effectuer les opérations techniques permettant d'obtenir la version en clair desdites données.

Lorsqu'un moyen de cryptographie a été utilisé, les autorités judiciaires peuvent exiger la convention secrète de déchiffrement du cryptogramme.

Article 85 : La réquisition prévue à l'article 84 ci-dessus peut être faite à tout expert. Dans ce cas, son exécution est faite conformément aux dispositions du Code de procédure pénale relatives à la commission d'expert.

Article 86 : Les autorités judiciaires peuvent donner commission rogatoire tant nationale qu'internationale, à toute personne morale ou physique pour rechercher les éléments constitutifs des infractions de cybercriminalité, dont au moins l'un des éléments constitutifs a été commis sur le territoire national ou dont l'un des auteurs ou complices se trouve sur ledit territoire.

Sous réserve des règles de réciprocité entre le Gabon et les pays étrangers liés par un accord de coopération judiciaire, les commissions rogatoires sont exécutées conformément aux dispositions des textes en vigueur.

Article 87 : Les personnes physiques ou morales qui fournissent des prestations de cryptographie visant à assurer une fonction de confidentialité, sont tenues de remettre aux Officiers de Police Judiciaire, sur présentation d'une réquisition, les conventions permettant le déchiffrement des données transformées au moyen des prestations qu'elles ont fournies.

Les Officiers de Police Judiciaire peuvent demander aux fournisseurs des prestations visées à l'alinéa 1er ci-dessus de mettre eux-mêmes en œuvre ces conventions.

Article 88 : Lorsque les nécessités de l'enquête ou de l'instruction le justifient, l'audition ou l'interrogatoire d'une personne ou la confrontation entre plusieurs personnes, peuvent être effectuées en plusieurs points du territoire national se trouvant reliés par des moyens de communications électroniques garantissant la confidentialité de la transmission.

Dans chacun des lieux, un Procès-verbal des opérations effectuées est dressé. Ces opérations peuvent faire l'objet d'enregistrement audiovisuel ou sonore.

Lorsque les circonstances l'exigent, l'interprétation peut être faite au cours d'une audition, d'un interrogatoire ou d'une confrontation par des moyens de communications électroniques.

Les modalités d'application du présent article sont définies par voie réglementaire.

Titre V : De la coopération judiciaire internationale

Article 89 : L'autorité ministérielle compétente peut, sous réserve de réciprocité, fournir sur demande d'une autorité ministérielle compétente étrangère, l'entraide judiciaire en vue de la recherche et la constatation des infractions pénales prévues par la présente loi.

L'entraide judiciaire concerne notamment les mesures de perquisition, de saisie, d'exécution de commission rogatoire internationale ou de conservation du système d'information ou de données.

Article 90 : La demande d'entraide précise notamment :

-l'autorité ministérielle compétente requérante ;
-l'infraction faisant l'objet de l'enquête ou des poursuites, ainsi qu'un exposé des faits ;
-le système d'information ou les données informatiques faisant l'objet de la demande de perquisition, de saisie ou de conservation et leur relation avec l'infraction ;
-toutes les informations disponibles pour identifier la personne visée ;
-la nécessité des mesures de perquisition, de saisie ou de conservation du système d'information ou de données concernés.

Article 91 : Les demandes d'entraide émanant des autorités judiciaires gabonaises et adressées aux autorités judiciaires étrangères sont transmises par l'intermédiaire du Ministère en charge des Affaires Etrangères.

Les pièces de la procédure sont transmises aux autorités de l'Etat requérant par la même voie.

Article 92 : Les demandes d'entraide émanant des autorités judiciaires étrangères sont adressées au Ministère en charge de la Justice qui saisit le Procureur Général compétent par l'intermédiaire du Ministre des Affaires Etrangères.

Article 93 : L'irrégularité formelle de la transmission de la demande d'entraide ne peut constituer une cause de nullité des actes accomplis en exécution de cette demande.

Article 94 : Lorsque l'exécution d'une demande d'entraide émanant d'une autorité judiciaire étrangère est de nature à porter atteinte à l'ordre public, à la défense, à la sécurité et aux intérêts de l'Etat, le Ministre chargé de la Justice notifie l'autorité requérante de ce qu'il ne peut être donné suite à sa demande.

Article 95 : Les autres modalités de mise en œuvre de la procédure d'entraide judiciaire sont fixées par les textes en vigueur.

Titre VI : Des dispositions diverses, transitoires et finales

Article 96 : Les propriétaires des plateformes et moteurs de recherches sont autorisés à supprimer ou à déréférencer les contenus signalés ou révélés comme manifestement illicites.

Article 97 : L'autorité administrative compétente peut adhérer aux organismes régionaux et internationaux œuvrant dans le domaine de la lutte contre la cybercriminalité à des fins de cohésion et d'efficacité des actions.

Article 98 : Toute personne physique ou morale concernée par les dispositions de la présente loi, dispose d'un délai maximum de six mois à compter de sa date d'entrée en vigueur pour s'y conformer, sous peine de sanctions.

Article 99 : Des textes législatifs et réglementaires déterminent en tant que de besoin, les dispositions de toute nature, nécessaires à l'application de la présente loi.

Article 100 : La présente loi, qui abroge toutes dispositions antérieures contraires, sera enregistrée, publiée au Journal Officiel et exécutée comme loi de la République.

Fait à Libreville, le 12 juillet 2023

Le Président de la République,
Chef de l'Etat

Ali BONGO ONDIMBA

Le Premier Ministre, Chef du Gouvernement
Alain-Claude BILIE-BY-NZE

Le Ministre d'Etat, Ministre de l'Intérieur
Lambert Noël MATHA

Le Ministre de l'Economie Numérique
Jean Pierre DOUKAGA-KASSA

Le Ministre de la Défense Nationale
Félicité ONGOUORI NGOUBILI

Le Ministre de la Justice, Garde des Sceaux et chargé des Droits de l'Homme
Erlyne Antonela NDEMBET épouse DAMAS

Le Ministre de l'Economie et de la Relance.
Nicole Jeanine Lydie ROBOTY épouse MBOU

_____

Loi n°033/2023 du 15 juillet 2023 modifiant et complétant certaines dispositions de la loi n°07/96 du 12 mars 1996 portant dispositions communes à toutes les élections politiques

L'Assemblée Nationale et le Sénat ont délibéré et adopté,
Le Président de la République, Chef de l'Etat,
Promulgue la loi dont la teneur suit :

Article 1er : La présente loi, prise en application des dispositions de l'article 47 de la Constitution, modifie et complète certaines dispositions de la loi no07/96 du 12 mars 1996 portant dispositions communes à toutes les élections politiques.

Article 2 : Les dispositions des articles 11, 15, 59, 68, 76, 77, 79, 90, 95, 102, 104, 105, 108 et 128, de la loi n°07/96 du 12 Mars 1996 portant dispositions communes à toutes les élections politiques sont modifiées, complétées et se lisent désormais ainsi qu'il suit :

« **Article 11 alinéa 4 nouveau** : En cas d'élections couplées ou générales, les commissions électorales mises en place administrent l'ensemble des scrutins. ».

« **Article 15 nouveau** : L'assemblée plénière est, en période électorale, l'instance de décision du Centre Gabonais des Elections.

En cas d'urgence, seuls les membres du bureau statuent.

En période normale, les décisions sont prises par les membres du bureau à la majorité simple.

Le mode de prise de décision au sein du Centre Gabonais des Elections est le consensus ou, à défaut, le vote à bulletin secret. Dans ce cas, seuls les membres du bureau participent au vote.

En cas d'égalité de voix, celle du président est prépondérante. ».

« **Article 59 alinéa 2 et 3 nouveau** : Toutefois, le Centre Gabonais des Elections peut, à titre exceptionnel, recevoir des déclarations de candidatures autres que celles du Président de la République.

Les candidatures ainsi enregistrées doivent être diffusées par tout moyen et affichées au siège de la commission électorale locale compétente.»

« **Article 68 nouveau** : Les modalités relatives au bulletin de vote arrêtées par le Centre Gabonais des Elections font l'objet d'un décret du Président de la République, pris sur proposition du Ministre de l'Intérieur. ».

« **Article 76 nouveau alinéas 9, 10 et 11** : En cas de pluralité de listes ou de candidats, ceux-ci sont représentés dans le bureau de vote par deux électeurs désignés à parité par les partis ou groupements de partis politiques légalement reconnus de la majorité et les partis ou groupements de partis politiques légalement reconnus de l'opposition présentant des candidats.

Les candidats ou listes de candidats indépendants sont représentés par un seul électeur désignés par eux.

Ces représentants dont les identités sont relevées avant l'ouverture du scrutin, doivent être munis d'un mandat écrit et ne sont pas membres du bureau de vote. Ils ont le statut d'observateur, leurs observations sont consignées dans le procès-verbal. ».

« **Article 77 nouveau** : L'urne électorale est transparente, numérotée et dispose d'une ouverture destinée à laisser passer l'enveloppe.

Avant le début du scrutin, l'urne doit être vidée de tout objet et présentée ouverte par le président du bureau de vote aux autres membres et aux représentants des candidats ou des listes de candidats. Elle est ensuite refermée à l'aide de deux serrures dont les clés restent l'une, entre les mains du président du bureau, l'autre entre les mains de l'assesseur le plus âgé.

L'urne électorale est placée en évidence devant les membres du bureau de vote.

A côté de l'urne, sont mis à la disposition des électeurs, la présente loi, les textes particuliers relatifs au vote, l'encreur ainsi que la liste électorale du bureau de vote.

Une liste d'émargement donnant les noms et prénoms des électeurs et le numéro de leurs cartes d'électeur, le tout conforme à la liste électorale du bureau de vote, est mise à la disposition d'un assesseur.

Chaque électeur est tenu de signer la liste d'émargement, de marquer un de ses doigts à l'encre indélébile et d'y apposer son empreinte digitale.

En cas d'élections couplées ou générales, le vote s'effectue dans un même bureau de vote.»

« **Article 79 nouveau** : Le vote a lieu sous enveloppe non transparente.

Le jour du vote, cette enveloppe est mise à disposition de chaque électeur dans la salle du scrutin.

Avant l'ouverture du scrutin, le bureau doit s'assurer que le nombre de bulletins et d'enveloppes pour chaque candidat ou liste de candidats est égal ou supérieur à celui des électeurs inscrits.

Au cas où il est constaté que le stock de bulletins pour un candidat ou une liste de candidats est incomplet, les opérations de vote ne peuvent démarrer. Le scrutin ne peut s'ouvrir qu'après reconstitution des stocks, et mention doit être portée au procès-verbal.

Le nombre de bulletins doit être le même pour tous les candidats.

Les bulletins sont remis à chaque électeur par l'un ou l'autre des deux assesseurs du bureau de vote.

Les deux assesseurs sont également chargés l'un, de remettre les bulletins de vote à l'électeur et, l'autre, de procéder à la vérification du nombre des bulletins remis.»

« **Article 90 alinéa 1 nouveau** : Tout représentant d'un candidat appartenant au camp de la majorité, de l'opposition, des indépendants dûment mandaté, a le droit de suivre les diverses opérations de vote. Tout représentant d'un camp dûment mandaté, a le droit de suivre les opérations de dépouillement de bulletins et de décompte de voix. Toutes observations formulées par lui doivent être consignées au procès-verbal. »

« **Article 95 nouveau** : Le vote doit s'accomplir dans la sérénité. L'entrée des électeurs dans la salle de vote avec une arme est interdite.

Le vote est unique : l'électeur ne peut disposer que d'une enveloppe.

Le vote est secret.

L'usage de l'isoloir est obligatoire, l'électeur s'y soustrait à la vue du public afin d'introduire dans l'enveloppe, le bulletin de son choix. Le reste des bulletins est déposé dans la poubelle présente dans l'isoloir.

L'électeur s'approche du président du bureau, lui fait constater qu'il n'est porteur que d'une seule enveloppe et lui présente sa carte d'électeur ou l'une des pièces prévues à l'article 54 ci-dessus. »

« **Article 102 nouveau** : Le mandataire participe au scrutin dans les conditions prévues à l'article 100 ci-dessus.

A son entrée dans la salle du scrutin, le mandataire doit présenter sa carte d'électeur, la procuration ainsi que la carte d'électeur du mandant.

Il lui est remis une enveloppe. Son vote est constaté par l'estampillage de la procuration et de la carte d'électeur du mandant ou l'une des pièces de ce dernier prévue à l'article 54 ci-dessus.

Le mandataire appose sa signature sur la liste d'émargement en face du nom du mandant.

La procuration est annexée au procès-verbal des opérations électorales. »

« **Article 104 nouveau** : Le dépouillement est public. Il est effectué sans interruption au lieu du vote par les membres du bureau en présence des représentants des candidats ou des listes de candidats.

L'un des vice-présidents ouvre l'enveloppe et l'autre lit le bulletin, les assesseurs inscrivent sur une feuille de dépouillement le décompte de voix exprimées dans l'enveloppe. »

« **Article 105 nouveau** : Une fois les opérations de vote terminées, le bureau de vote procède à la comptabilisation de tous les votes et en dresse procès-verbal. »

Sont comptabilisés comme nuls :

-les bulletins blancs ;
-les bulletins sur lesquels le votant s'est fait connaitre ;
-les bulletins trouvés sans enveloppe ou dans des enveloppes non réglementaires ;
-les bulletins multiples et contradictoires placés dans l'enveloppe ;
-les bulletins sur lesquels le nom d'un ou plusieurs candidats a été rayé ou ajouté. ».

« **Article 108 nouveau** : Immédiatement après la fin du dépouillement, le procès-verbal des opérations électorales est rédigé en sept exemplaires destinés aux

commissions électorales et en deux exemplaires remis aux représentants de chaque camp politique, de la majorité, de l'opposition ainsi que celui des indépendants de la circonscription électorale concernée. Celui-ci est signé des assesseurs, des vice-présidents et du président. Les bulletins déclarés nuls y sont annexés ainsi que la liste des émargements des votes, des feuilles de dépouillement du scrutin ou toutes autres pièces relatives aux incidents du scrutin.

Les résultats sont immédiatement annoncés au public par le président du bureau de vote qui remet séance tenante les exemplaires des procès-verbaux aux représentants des candidats de chaque camp politique et des candidats indépendants, tel que prévu à l'article 76 ci-dessus.

Les résultats indiquent le nombre et le pourcentage des voix obtenus par chaque candidat et par chaque liste par rapport à l'ensemble des voix valablement exprimées. »

« **Article 128 nouveau** : Constituent des causes d'annulation totale ou partielle des élections :

-la constatation de l'inéligibilité d'un candidat ;
-l'existence d'une candidature multiple ;
-l'organisation des élections en dehors des circonscriptions ou sections électorales définies par la loi ;
-l'organisation du scrutin dans les lieux autres que les bureaux de vote réguliers ;
-le défaut d'isoloir dans un bureau de vote, même hors de toute intention de fraude ;
-le déplacement de l'urne hors du bureau de vote avant ou pendant le dépouillement sans l'autorisation du bureau de vote ;
-la constatation dans l'urne d'un nombre d'enveloppes supérieur au nombre d'émargements ;
-la manipulation avérée du fichier électoral ou de la liste électorale ;
-l'arrêt définitif des opérations de vote pour insuffisance de bulletins de vote. ».

Article 3 : La présente loi, qui abroge toutes les dispositions antérieures contraires, sera enregistrée, publiée selon la procédure d'urgence et exécutée comme loi de la République.

Fait à Libreville, le 15 juillet 2023

Le Président de la République,
Chef de l'Etat

Ali BONGO ONDIMBA

Le Premier Ministre, Chef du Gouvernement
Alain-Claude BILIE-BY-NZE

Le Ministre d'Etat, Ministre de l'Intérieur
Lambert-Noël MATHA

Le Ministre de la Justice, Garde des Sceaux et chargé des Droits de l'Homme
Erlyne Antonela NDEMBET EP. DAMAS

Le Ministre du Budget et des Comptes Publics
Edith EKIRI MOUNOMBI EP. OYOUOMI

PRESIDENCE DE LA REPUBLIQUE

Décret n°166/PR du 12 juillet 2023 portant promulgation de la loi n°025/2023 portant modification de la loi n°001/2011 du 25 septembre 2011 relative à la protection des données à caractère personnel

LE PRESIDENT DE LA REPUBLIQUE,
CHEF DE L'ETAT ;

Vu la Constitution, notamment en son article 17, alinéa 1er ;

D E C R E T E :

Article 1er : Est promulguée la loi n°025/2023 portant modification de la loi n°001/2011 du 25 septembre 2011 relative à la protection des données à caractère personnel.

Article 2 : Le présent décret sera enregistré, publié au Journal Officiel et communiqué partout où besoin sera.

Fait à Libreville, le 12 juillet 2023

Par le Président de la République,
Chef de l'Etat

Ali BONGO ONDIMBA

Décret n°167/PR du 12 juillet 2023 portant promulgation de la loi n°026/2023 autorisant l'Etat Gabonais à contracter un emprunt d'un montant équivalent à cinquante millions (50.000.000) de dollars US auprès de la Banque Arabe pour le Développement Economique en Afrique (BADEA)

LE PRESIDENT DE LA REPUBLIQUE,
CHEF DE L'ETAT ;

Vu la Constitution, notamment en son article 17, alinéa 1er ;

D E C R E T E :

Article 1er : Est promulguée la loi n°026/2023 autorisant l'Etat Gabonais à contracter un emprunt d'un montant équivalent à cinquante millions (50.000.000) de dollars US auprès de la Banque Arabe pour le Développement Economique en Afrique (BADEA).

Article 2 : Le présent décret sera enregistré, publié au Journal Officiel et communiqué partout où besoin sera.

Fait à Libreville, le 12 juillet 2023

Par le Président de la République,
Chef de l'Etat

Ali BONGO ONDIMBA

_____

Décret n°168/PR du 12 juillet 2023 portant promulgation de la loi n°027/2023 portant règlementation de la cybersécurité et de la lutte contre la cybercriminalité en République Gabonaise

LE PRESIDENT DE LA REPUBLIQUE,
CHEF DE L'ETAT ;

Vu la Constitution, notamment en son article 17, alinéa 1er ;

D E C R E T E :

Article 1er : Est promulguée la loi n°027/2023 portant règlementation de la cybersécurité et de la lutte contre la cybercriminalité en République Gabonaise.

Article 2 : Le présent décret sera enregistré, publié au Journal Officiel et communiqué partout où besoin sera.

Fait à Libreville, le 12 juillet 2023
Par le Président de la République,
Chef de l'Etat

Ali BONGO ONDIMBA

_____

Décret n°169/PR du 15 juillet 2023 portant promulgation de la loi n°033/2023 modifiant et complétant certaines dispositions de la loi n°07/96 du 12 mars 1996 modifiée portant dispositions communes à toutes les élections politiques

LE PRESIDENT DE LA REPUBLIQUE,
CHEF DE L'ETAT ;

Vu la Constitution, notamment en son article 17, alinéa 1er ;

D E C R E T E :

Article 1er : Est promulguée la loi n°033/2023 modifiant et complétant certaines dispositions de la loi n°07/96 du 12 mars 1996 modifiée portant dispositions communes à toutes les élections politiques

Article 2 : Le présent décret sera enregistré, publié au Journal Officiel et communiqué partout où besoin sera.

Fait à Libreville, le 15 juillet 2023

Par le Président de la République,
Chef de l'Etat

Ali BONGO ONDIMBA

_____

MINISTERE DE L'INTERIEUR

_____

Décret n°165/PR/MI du 12 juillet 2023 portant modification de l'article 2 du décret n°0148/PR/MI du 3 juillet 2023 fixant la date limite de dépôt des déclarations de candidature pour l'élection du Président de la République, l'élection des députés à l'Assemblée Nationale et l'élection des membres des conseils départementaux et des conseils municipaux de l'année 2023

Le Président de la République,
Chef de l'Etat ;
Vu la Constitution ;
Vu la loi n°07/96 du 12 mars 1996 portant dispositions communes à toutes les élections politiques, ensemble les textes modificatifs subséquents ;
Vu la loi organique n°10/96 du 15 avril 1996 relative aux conditions d'éligibilité du Président de la République, modifiée par l'ordonnance n°16/98 du 14 août 1998 ;
Vu la loi n°16/96 du 15 avril 1996 portant dispositions spéciales relatives à l'élection du Président de la République, modifiée par la loi n°11/2004 du 06 janvier 2005 ;
Vu la loi n°11/96 du 15 avril 1996 relative à l'élection des députés à l'Assemblée Nationale, ensemble les textes modificatifs subséquents ;
Vu la loi n°15/96 du 15 avril 1996 portant dispositions spéciales relatives à l'élection des députés à l'Assemblée Nationale, ensemble les textes modificatifs subséquents ;
Vu la loi n°19/96 du 15 avril 1996 relative à l'élection des membres des Conseils départementaux et des Conseils municipaux ;
Vu le décret n°0818/PR/MISPID du 24 septembre 2013 fixant le nombre des membres des bureaux des Conseils départementaux, des Conseils municipaux et des Conseils d'arrondissement ;
Vu le décret n°0819/PR/MISPID du 24 septembre 2013 fixant le nombre des membres des Conseils départementaux, des Conseils municipaux et des Conseils d'arrondissement ;
Vu le décret n°0007/PR/MI du 13 février 2023 portant composition du Bureau du Centre Gabonais des Elections ;
Vu le décret n°0333/PR/MISPID du 28 février 2013 portant attributions et organisation du Ministère de l'Intérieur, de la Sécurité Publique, de l'Immigration et de la Décentralisation ;
Vu le décret n°0001/PR du 09 janvier 2023 portant nomination du Premier Ministre, Chef du Gouvernement ;

Vu le décret n°0003/PR/PM du 09 janvier 2023 fixant la composition du Gouvernement de la République, modifié par le décret n°0046/PR/PM du 26 avril 2023 portant réaménagement du Gouvernement de la République ;

Le Conseil d'Etat consulté ;
Le Conseil des Ministres entendu ;

D E C R E T E :

Article 1er : Le présent décret, pris en application des dispositions des articles 59 de la loi n°07/96 du 12 mars 1996, modifiée, 11 de la loi organique n°16/96 du 15 avril 1996 et 6 de la loi organique n°11/96 du 15 avril 1996, susvisées, modifie l'article 2 du décret n°0148/PR/MI du 3 juillet 2023 fixant la date limite de dépôt des déclarations de candidature pour l'élection du Président de la République, l'élection des députés à l'Assemblée Nationale et de l'élection des membres des conseils départementaux et des conseils municipaux de l'année 2023.

« **Article 2 nouveau** : La date limite de dépôt des déclarations de candidature à l'élection du Président de la République, à l'élection des députés à l'Assemblée Nationale et à l'élection des membres des conseils départementaux et des conseils municipaux, visée à l'article 1er ci-dessus est fixée au dimanche 16 juillet 2023 à 18 heures. »

Article 3 : Le présent décret qui prend effet à compter de sa date de signature sera enregistré, publié au Journal Officiel et communiqué partout où besoin sera.

Fait à Libreville, le 12 juillet 2023

Par le Président de la République,
Chef de l'Etat ;
Ali BONGO ONDIMBA.

Le Premier Ministre, Chef du Gouvernement
Alain-Claude BILIE-By-NZE

Le Ministre d'Etat, Ministre de l'Intérieur
Lambert-Noël MATHA

Le Ministre du Budget et des Comptes Publics
Edith EKERI MOUNOMBI ép. OYOUOMI

_____

_____

Je désire m'abonner au Journal Officiel pendant :

Six (6) mois ☐ Un (1) an ☐ —— Particulier ☐ Entreprise ☐ Administration ☐

Nom :..... Prénoms :.....

Raison Sociale :.....

Ville :..... Pays :..... Boite postale :..... Tél.:.....

E-mail: .....

Mode de Règlement :

- Chèque ☐
- Espèces ☐
- Mandat express ☐
- Virement ☐

Date :

Signature :

DESTINATIONS	1 an (en FCFA)	6 mois (en FCFA)
Libreville	26.000	13.000
Intérieur Gabon	28.000	14.000
Afrique équatoriale, Nigeria, Zaïre	30.000	15.000
Autres pays d'Afrique noire francophone	31.000	15.000
Autre pays d'Afrique	32.000	16.000
France	32.000	16.000
Europe	36.000	18.000
Amérique, Moyen-Orient	40.000	20.000
Asie, Océanie	42.000	21.000

BULLETIN A DECOUPER ET A RENVOYER A LA DIRECTION DES PUBLICATIONS OFFICIELLES
405, AVENUE COLONEL PARANT
BP 563 LIBREVILLE / TEL (+241) 72 01 04