TABLE DES MATIERES

Livre Préliminaire : Dispositions générales

Chapitre unique : Dispositions préliminaires

Article 1 Définitions

Abonné : toute personne physique ou morale ayant souscrit à une offre de service avec un opérateur ou un fournisseur d'accès.

Accès (au sens du Livre Deuxième sur les communications électroniques) : mise à disposition d'infrastructures passives ou actives, de moyens, matériels ou logiciels, ou de services, en vue de permettre au bénéficiaire d'exploiter un réseau de communications électroniques ou de fournir des services de communications électroniques, y compris les prestations associées telle que la colocalisation.

Accès (au sens du Livre Troisième sur la cryptologie) : capacité et manière de communiquer ou d'interagir avec un système, d'utiliser les ressources d'un système pour traiter des informations, de prendre connaissance des informations contenues dans le système ou de contrôler les composantes et les fonctions d'un système.

Adresse IP : étiquette numérique attribuée à tout appareil connecté à un réseau informatique qui utilise le protocole Internet pour la communication. Une adresse IP remplit deux fonctions principales : l'identification de l'hôte ou de l'interface réseau et l'adressage de l'emplacement.

Administration : les administrations de l'Etat, les collectivités territoriales, leurs établissements publics administratifs et les organismes et personnes de droit public et de droit privé chargés d'une mission de service public ou de la gestion d'un service public.

Affectataire (de fréquences radioélectriques) : administration, département ministériel, établissement public ou autorité indépendante se voyant attribuer une ou plusieurs bandes de fréquences dans le tableau national d'attribution des bandes de fréquences pour son propre usage ou en vue de l'assignation de fréquences à des tiers.

Assignation (d'une fréquence radioélectrique) : autorisation donnée par un affectataire pour l'utilisation par une station radioélectrique d'une fréquence ou d'un canal radioélectrique déterminé selon des conditions spécifiées.

Attribution (d'une bande de fréquences radioélectriques) : inscription dans le tableau national d'attribution des bandes de fréquences d'une bande de fréquences déterminée aux fins de son utilisation par un ou plusieurs services de radiocommunication de terre ou spatiaux dans des conditions spécifiées. Ce terme s'applique également à la bande de fréquences considérée.

Attestation électronique : Document d'identité numérique dont l'objet est d'identifier une entité physique ou non physique. Le certificat numérique ou électronique est un lien entre l'entité physique et l'entité numérique (virtuel).

Autorité de régulation : désigne l'Autorité de régulation multisectorielle de Djibouti créée par la loi n° 74/AN/20/8ème L du 13 février 2020 portant création de l'Autorité de régulation multisectorielle de Djibouti.

Boucle locale ou sous-boucle locale : circuit physique qui relie les points de terminaison d'un réseau de communications électroniques dans les locaux des utilisateurs finals au répartiteur principal ou à toute autre installation équivalente du réseau de communications électroniques d'un opérateur.

Brouillage préjudiciable : le brouillage qui compromet le fonctionnement d'un service de radionavigation ou d'autres services de sécurité ou qui, d'une autre manière, altère gravement, entrave ou interrompt de façon répétée le fonctionnement d'un service de radiocommunications opérant conformément au Règlement des radiocommunications de l'Union internationale des télécommunications et aux dispositions du présent Code et aux textes pris pour son application.

Cachet électronique : données électroniques, jointes ou associées logiquement à d'autres données électroniques afin de garantir l'origine et l'intégrité de ces dernières.

Cachet électronique avancé : cachet électronique qui satisfait aux exigences énoncées à l'Article 447.

Cachet électronique qualifié : cachet électronique qui satisfait aux exigences fixées à l'Article 448.

Certificat d'authentification de site Internet : attestation permettant d'authentifier un site internet et l'associant à la personne physique ou morale à laquelle le certificat est délivré.

Carte SIM (*Subscriber Identity Module*) : un circuit intégré destiné à stocker de manière sécurisé le numéro d'identification international d'un utilisateur de services téléphoniques mobiles et sa clé associée, utilisés pour identifier et authentifier les utilisateurs et leurs équipements sur les réseaux de communications électroniques mobiles.

Certificat d'authentification de site Internet qualifié : certificat d'authentification de site Internet délivré par un prestataire de services de confiance qualifié, et qui satisfait aux exigences fixées à l'Article 475.

Certificat de cachet électronique : attestation électronique qui associe les données de validation d'un cachet électronique à une personne morale et confirme le nom de cette personne.

Certificat de cachet électronique qualifié : certificat de cachet électronique délivré par un prestataire de services de confiance qualifié.

Certificat de signature électronique : attestation électronique qui associe les données de validation d'une signature électronique à une personne physique et confirme au moins le nom de cette personne.

Certificat qualifié de signature électronique: certificat de signature électronique qui satisfait aux exigences fixées à l'Article 436.

Chiffrement : toute technique qui consiste à transformer des données numériques en un format inintelligible en employant des moyens de cryptologie.

Clé privée : le processus qui permet de déchiffrer des données.

Clé publique : le processus qui permet de chiffrer des données.

Code source : tout code écrit dans un langage de programmation et qui peut être converti pour constituer un programme exécutable.

Commerce électronique : l'acte d'offrir, d'acheter, ou de fournir des biens et des services via les systèmes informatiques et les réseaux de communications électroniques.

Commission : désigne la Commission Nationale de Protection des Données à Caractère Personnel telle que ressortant des dispositions édictées au Chapitre premier : La Commission Nationale de Protection des Données à Caractère Personnel du Titre 4 du Livre Premier.

Colocalisation : prestation offerte par un opérateur à d'autres opérateurs et consistant en une mise à leur disposition d'infrastructures, y compris des locaux, afin qu'ils y installent leurs équipements. Le terme colocalisation couvre également les prestations de colocalisation offertes dans un bâtiment aménagé à cet effet adjacent ou distant du point de terminaison objet d'un accord d'accès et/ou d'interconnexion.

Commanditaire : désigne toute personne désirant fournir un ou plusieurs services de confiance qualifiés.

Communications électroniques : toute émission, transmission ou réception de signes, de signaux, d'écrits, d'images, de sons par voie électromagnétique.

Communication au public en ligne : toute transmission, sur demande individuelle, de données numériques n'ayant pas un caractère de correspondance privée, par un procédé de communication électronique permettant un échange réciproque d'informations entre l'émetteur et le récepteur.

Communication au public par voie électronique : toute mise à disposition au public ou à des catégories de public, par un procédé de communication électronique, de signes, signaux, écrits, images, sons ou messages de toute nature qui n'ont pas le caractère d'une correspondance privée.

Convention secrète de déchiffrement : les 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.

Consommateur : tel que défini à l'article L. 2211-102 du code de commerce, *« toute personne qui agit à des fins qui n'entrent pas dans le cadre d'une activité professionnelle »*.

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

Cryptographie : L'étude des moyens et produits de chiffrement permettant de rendre illisible des informations afin de garantir l'accès à un seul destinataire authentifié.

Cryptage : Utilisation de code ou signaux non usuels permettant la conservation des informations à transmettre en des signaux incompréhensibles par les tiers.

Code de conduite : Tout ensemble de règles notamment les chartes d'utilisation élaborés par les responsables du traitement, en conformité avec le présent codeafin d'instaurer un usage correct des ressources informatiques, de l'internet et des communications électroniques de la république de Djibouti.

Consentement : Toute manifestation de volonté expresse, non équivoque et libre par laquelle la personne concernée ou son représentant légal accepte que ses données à caractère personnel fasse l'objet d'un traitement manuel ou électronique.

Copie temporaires : Données copiées temporairement dans un espace dédié pour une durée limitée dans le temps pour les besoins du fonctionnement du logiciel de traitement

Cybercriminalité : toutes les infractions pénales susceptibles de se commettre au moyen ou sur un réseau de communication électronique, ou d'un système informatique généralement connecté à un réseau de communication électronique.

Cybersécurité : ensemble des 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.

Déchiffrement : toute technique qui consiste à transformer des données numériques en un format intelligible en employant des moyens de cryptologie.

Dégroupage de la boucle locale : prestation d'accès qui inclut également les prestations associées, notamment celle de colocalisation, offerte par un opérateur pour permettre à un second opérateur d'accéder à tous les éléments de sa boucle locale exploitant pour desservir directement ses propres utilisateurs finals.

Demande : les demandes et les réclamations, y compris les recours gracieux ou hiérarchiques, adressées à l'administration.

Destinataire (d'un traitement de données à caractère personnel) : toute personne physique ou morale, publique ou privée, toute autre autorité publique ou tout autre organisme, qui reçoit communication de ces données autre que la personne concernée, le responsable de traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable de traitement ou du sous-traitant, sont chargées de traiter ces données. Toutefois, les autorités légalement habilitées, dans le cadre d'une mission particulière ou de l'exercice d'un droit de communication, à demander au responsable de traitement de leur communiquer des données à caractère personnel ne constituent pas des destinataires.

Déclaration : L'acte préalable au commencement des activités, émanant d'un operateur ou d'un fournisseur de services de communications électroniques et qui ne l'oblige pas à obtenir une décision explicite avant de commencer ses activités, de bénéficier des droits et d'être assujetti aux obligations découlant de cet acte.

Données sensibles : Toute information relative aux opinions ou activités religieuses, philosophiques, politiques, syndicales, à la vie sexuelle, à la race, à la sante, aux mesures d'ordre social, aux poursuites, aux sanctions pénales ou administratives.

Directeur de la publication : le représentant légal de l'entreprise éditrice. Dans le cas particulier des sociétés anonymes, le directeur de la publication est le président du directoire ou le directeur général unique.

Dispositif de création de signature électronique : tout dispositif, logiciel ou matériel servant à créer une signature électronique.

Dispositif qualifié de création de signature électronique : tout dispositif de création de signature électronique qui satisfait aux exigences fixées à l'Article 430.

Données à caractère personnel : toute information relative à une personne physique identifiée ou identifiable. Est considérée identifiable une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

Données biométriques : les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales, des données dactyloscopiques, des empreintes vocales, l'ADN, de l'iris ou de la rétine.

Données de création de signature électronique : des données uniques qui sont utilisées par le signataire pour créer une signature électronique.

Données de santé à caractère personnel : les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, qui révèlent des informations sur son état de santé.

Données de validation : données servant à valider une signature électronique.

Données d'identification personnelle : un ensemble de données permettant d'établir l'identité d'une personne physique ou morale, ou d'une personne physique représentant une personne morale.

Données génétiques : toute information concernant les caractères génétiques héréditaires ou acquis d'une personne physique qui donnent des indications uniques sur la physiologie ou l'état de santé de cette personne physique et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question.

Données informatisées : toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique.

Données relatives au trafic : toute donnée traitée en vue de l'acheminement d'une communication par un réseau de communications électroniques ou en vue de sa facturation, y compris toute donnée indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type de service sous-jacent.

Droit à l'effacement : le droit pour toute personne concernée d'obtenir du responsable de traitement l'effacement, dans les meilleurs délais, de ses données à caractère personnel, dans les conditions prévues aux Article 42 et suivants.

Equipement, installation ou réseau radioélectrique : tout équipement, installation ou réseau qui utilise intentionnellement des fréquences radioélectriques, en émission ou en réception, pour la propagation des ondes électromagnétiques en espace libre, à des fins de radiocommunication ou de radiorepérage, y compris les équipements permettant de recevoir des services de radio ou de télévision.

Équipement terminal : tout équipement destiné à être connecté directement ou indirectement à un point de terminaison d'un réseau de communications électroniques en vue de la transmission, du traitement ou de la réception d'informations.

Exigences essentielles : les exigences nécessaires pour garantir la préservation de l'intérêt général s'attachant :

1. à la protection de la santé, de la sécurité des personnes et des animaux domestiques ainsi que des biens ;

2. à la protection des réseaux de communications électroniques et notamment des échanges d'information de commande et de gestion qui y sont associées ;

3. à l'interopérabilité des services de communications électroniques, des réseaux de communications électroniques et des équipements terminaux ;

4. au maintien d'un niveau adéquat de compatibilité électromagnétique entre équipements et installations radioélectriques ;

5. à une utilisation efficace des fréquences radioélectriques par les équipements et à une contribution à l'utilisation optimisée de ces dernières en évitant des brouillages préjudiciables pour les tiers.

Exploitant d'infrastructures alternatives : toute personne physique ou morale qui détient, exploite ou assure la gestion d'infrastructures alternatives, sans exercer elle-même les activités d'opérateur.

Exploitant d'infrastructures passives : toute personne physique ou morale dont l'activité consiste exclusivement à détenir, exploiter et/ou assurer la gestion d'infrastructures passives, sans exercer elle-même les activités d'opérateur.

Fichier : tout ensemble structuré et stable de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique.

Fournisseurs d'accès : les fournisseurs d'accès désignent ceux dont l'activité est d'offrir un accès à des services de communication au public.

Fournisseurs de contenu : la personne qui détermine les contenus qui doivent être mis à la disposition du public sur le service qu'il a créé ou dont il a la charge.

Fournisseur de services en ligne : personne physique ou morale qui assure, même à titre gratuit, pour mise à disposition du public par des services de communications au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par les destinataires de ces services

Fournisseurs d'hébergement : les personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au

public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou des messages de toutes natures fournis par les destinataires de ces services.

Franc Djibouti ou DJF : monnaie officielle en République de Djibouti.

Gestionnaire du système national de données de santé : la personne physique ou morale responsable du système national de données de santé, de l'ensemble des composants matériels et logiciels du système national de données de santé, ainsi que du choix et de l'exploitation des services de télécommunications mis en œuvre pour le système national de données de santé, telle que désignée à l'Article 740 .

Hébergeur de données de santé : toute personne dont l'activité consiste à stocker et à donner accès à des données de santé recueillies à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi social ou médico-social, pour le compte de personnes physiques ou morales à l'origine de la production ou du recueil de ces données, ou pour le compte du patient lui-même.

Information sur le régime des droits : toute information fournie par les titulaires de droits qui permet d'identifier l'œuvre ou tout autre objet protégé, l'auteur ou autre titulaire de droits, les informations sur les conditions et modalités d'utilisation de l'œuvre ou autre objet protégé ainsi que tout numéro ou code représentant ces informations.

Infrastructures actives : équipements actifs de réseaux de communications électroniques, notamment les antennes, stations de base, contrôleurs de stations de base et liens de transmission associés.

Infrastructure alternative : tout élément ou ensemble d'éléments d'un réseau destiné à fournir un service dans le domaine de la production, du transport ou de la distribution d'électricité, y compris pour l'éclairage public, de gaz ou de chaleur, d'eau y compris d'évacuation ou de traitement des eaux usées, ou destiné à fournir des services de transport, y compris les voies ferrées, les routes, les ports et les aéroports, pouvant accueillir des éléments d'un réseau de communications électroniques sans devenir lui-même un élément actif du réseau de communications électroniques, tels que les conduites, pylônes, gaines, chambres de tirage et regards, trous de visite, boîtiers, immeubles ou accès à des immeubles, installations liées aux antennes, tours et poteaux, châteaux d'eau.

Infrastructure essentielle : toute infrastructure de communications électroniques passive ou active ou qui ne peut être reproduite dans des conditions économiques raisonnables et pour laquelle il n'existe pas de substitut réel ou potentiel permettant de fournir les mêmes services avec une qualité de service comparable ou des services sur un marché amont, aval ou connexe.

Infrastructure passive : toute infrastructure physique et autre ressource associée à un réseau de communications électroniques ou à un service de communications électroniques, qui concourt ou peut concourir à la fourniture de services via ce réseau ou ce service. Sont notamment considérés comme des infrastructures passives les bâtiments ou accès aux bâtiments, le câblage des bâtiments, tours et autres constructions de soutènement, les artères de génie civil aériennes et souterraines, les gaines, conduites, pylônes, trous de visite et boîtiers, adductions, cheminements en façade, cheminements aériens et poteaux ainsi que les équipements passifs de réseaux de communications électroniques, notamment les câbles de communications électroniques de toute nature, les éléments de branchement, d'interconnexion, d'alimentation et de climatisation.

Installation : tout équipement, appareil, câble, élément d'infrastructures et dispositifs électriques, systèmes radioélectriques ou optiques ou tout autre système technique pouvant servir aux technologies de l'information et de la communication ou à toute autre opération qui y est directement liée.

Interconnexion : forme particulière d'accès mises en œuvre entre opérateurs au moyen de la liaison physique et logique des réseaux de communications électroniques exploités par le même opérateur ou un opérateur différent, afin de permettre aux utilisateurs d'un opérateur de communiquer avec les utilisateurs du même opérateur ou d'un autre, ou d'accéder aux services de communications électroniques fournis par un autre opérateur lorsque ces services sont fournis par les parties concernées ou par d'autres parties qui ont accès aux réseaux de communications électroniques.

Intermédiaire technique : les intermédiaires techniques visés par la présente loi peuvent être répartis en trois catégories : les opérateurs, les fournisseurs d'hébergements et les fournisseurs d'accès.

Internet : Internet est un système de communications électroniques développé au niveau international qui permet d'accéder à des données de toutes sortes grâce à un codage universalisé.

Itinérance : prestation, forme particulière d'accès, fournie par un opérateur de réseau de communications électroniques ouvert au public mobiles à un autre en vue de permettre, sur une zone qui n'est pas couverte par le second, l'accueil des clients de ce dernier sur le réseau du premier.

Horodatage électronique : données sous forme électronique qui associent d'autres données sous forme électronique à un instant particulier et établissent la preuve que ces dernières données existaient à cet instant.

Horodatage électronique qualifié : horodatage électronique qui satisfait aux exigences fixées à l'Article 458.

Identification électronique : le processus consistant à utiliser des données d'identification personnelle sous une forme électronique, représentant de manière univoque une personne physique ou morale, ou une personne physique représentant une personne morale.

Loteries sur Internet : toutes opérations offertes au public sur Internet, sous quelque dénomination que ce soit, pour faire naître l'espérance d'un gain qui serait dû, même partiellement au hasard et pour lesquelles un sacrifice financier est exigé par l'opérateur de la part des participants.

Marché de détail : Le maillon final de la chaine de distribution. C'est-à-dire le marché sur lequel les biens sont transférés, ou les services sont fournis aux consommateurs finaux.

Marche de gros : Est un marché qui met en œuvre la pratique dite du commerce de gros. Par définition, le commerce de gros est une activité professionnelle qui relie les producteurs aux distributeurs et plus loin aux consommateurs.

Message : communication quelconque sous forme de parole, son, donnée, texte, image visuelle, signal ou code, ou toute autre forme ou combinaison de formes.

Mineur : toute personne physique âgée de moins de 18 ans au sens de la convention des Nations Unies sur les droits de l'enfant.

Moyen de cryptologie : tout matériel ou logiciel conçu ou modifié pour transformer des données, qu'il s'agisse d'informations ou de signaux, à l'aide de conventions secrètes ou pour réaliser l'opération inverse avec ou sans convention secrète. Les moyens de cryptologie ont principalement pour objet de garantir la sécurité du stockage ou de la transmission de données, en permettant d'assurer leur confidentialité, leur authentification ou le contrôle de leur intégrité.

Moyen d'identification électronique : élément matériel et/ou immatériel contenant des données d'identification personnelle et utilisé pour authentifier un utilisateur de services en ligne.

Numéro : toute chaîne de chiffres indiquant de façon univoque le point de terminaison d'un réseau de communications électroniques ouvert au public. Le numéro peut avoir un format national ou international. Le format international est connu comme le numéro de communication électronique publique internationale qui comporte l'indicatif du pays et les chiffres subséquents.

Ondes radioélectriques : ondes électromagnétiques se propageant dans l'espace sans guide artificiel. Les ondes radioélectriques peuvent également être désignées par leur fréquence, auquel cas il est fait référence aux fréquences radioélectriques.

Opérateur : toute personne physique ou morale exploitant un réseau de communications électroniques ouvert au public ou fournissant au public un service de communications électroniques.

Opérateur d'infrastructures : tout opérateur fournissant exclusivement des services de communications électroniques aux autres opérateurs sur le marché de gros.

Opérateur de réseau mobile virtuel : tout opérateur ne possédant pas d'installations ou de réseau radioélectriques qui utilise le réseau de communications électroniques ouvert au public mobile d'un ou plusieurs opérateurs afin de fournir à ses utilisateurs des services téléphoniques mobiles.

Opérateur non national : tout opérateur dûment autorisé à exercer des activités de communications électroniques dans un autre Etat que la République de Djibouti et ne bénéficiant pas du droit d'exploiter un réseau de communications électroniques ou de fournir des services de communications électroniques au titre du présent Code.

Paiement mobile : toute opération réalisée par un instrument permettant à une personne d'obtenir de l'argent, des biens ou des services, d'effectuer des paiements, ou de transférer de l'argent, par un dispositif de téléphonie mobile.

Personne concernée : la personne à laquelle se rapportent les données à caractère personnel qui font l'objet d'un traitement.

Point de terminaison d'un réseau : le point physique auquel un utilisateur final obtient l'accès à un réseau de communications électroniques ouvert au public et qui est, dans le cas de réseaux utilisant la commutation et l'acheminement, identifié par une adresse réseau spécifique, qui peut être rattachée au numéro ou au nom d'un utilisateur final. Ce point fait partie intégrante du réseau et ne constitue pas en soi un réseau de communications électroniques. Lorsqu'un réseau de communications électroniques est connecté à un réseau étranger, les points de connexion à ce réseau sont considérés comme des points de terminaison. En cas de réseaux de radiocommunications, les interfaces aériennes des équipements terminaux mobiles sont considérées comme points de terminaison.

Pornographie infantile : toute représentation visuelle d'un comportement sexuellement explicite y compris toute photographie, film, vidéo, image que ce soit fabriquée ou produite par voie électronique, mécanique ou par autres moyens où la production de telles représentations visuelles implique un mineur ; ces représentations visuelles sont une image numérique, une image d'un ordinateur ou une image générée par un ordinateur où un mineur est engagé dans un comportement sexuellement explicite ou lorsque des images de leurs organes sexuels sont produites ou utilisées à des fins principalement sexuelles et exploitées à l'insu de l'enfant ou non ; cette représentation visuelle a été créée, adaptée ou modifiée pour qu'un mineur engage dans un comportement sexuellement explicite.

Prestataire de services de confiance : une personne physique ou morale qui fournit un ou plusieurs services de confiance.

Prestataire de services de confiance qualifié : un prestataire de services de confiance qui fournit un ou plusieurs services de confiance et qui satisfait aux exigences fixées à l'Article 409.

Prestation de cryptologie : toute opération visant à la mise en œuvre, pour le compte d'autrui, de moyens de cryptologie.

Professionnel : toute personne physique ou morale qui, pour les pratiques commerciales relevant du Livre Quatrième, agit à des fins qui entrent dans le cadre de son activité commerciale, industrielle, artisanale ou libérale, et toute personne agissant au nom ou pour le compte d'une telle personne.

Professionnels et services sociaux ou médico-sociaux : professionnel ou établissement dont les activités portent sur l'évaluation et la prévention des risques sociaux et médico-sociaux, relatifs notamment à l'enfance, à l'éducation, à l'assistance dans les divers actes de la vie, au soutien, et à l'accompagnement du développement social.

Prospection directe : toute sollicitation effectuée au moyen de l'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 ou une action politique ou caritative.

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

Public : toute personne physique ou toute personne morale de droit privé, à l'exception de celles qui sont chargées d'une mission de service public lorsqu'est en cause l'exercice de cette mission.

Publicité : ensemble de procédés et de moyens destinés à la communication institutionnelle ou à la promotion commerciale d'un produit ou d'un service par tout média, tout format ou tout support de communication.

Radiocommunication : toute émission, transmission ou réception d'ondes radioélectriques à des fins spécifiques de communications électroniques.

Raciste et xénophobe en matière des technologies de l'information et de la communication : tout écrit, toute image ou toute autre représentation d'idées ou de théories 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 l'ascendance ou de l'origine nationale ou ethnique ou de la religion, dans la mesure où cette dernière sert de prétexte à l'un ou l'autre de ces éléments ou qui incite à de tels actes.

Réseau de communications électroniques : les systèmes de transmission, qu'ils soient ou non fondés sur une infrastructure permanente ou une capacité d'administration centralisée et, le cas échéant, les équipements de commutation ou de routage et les autres éléments, y compris les éléments de réseau qui ne sont pas actifs, qui permettent l'acheminement de signaux par câble, par la voie hertzienne, par moyen optique ou par d'autres moyens électromagnétiques, comprenant les réseaux satellitaires, les réseaux fixes (avec commutation de circuits ou de paquets, y compris l'Internet) et mobiles, les systèmes utilisant le réseau électrique, pour autant qu'ils servent à la transmission de signaux, les réseaux utilisés pour la radiodiffusion sonore et télévisuelle et les réseaux câblés de télévision, quel que soit le type d'information transmise.

Réseau de communications électroniques ouvert au public : réseau de communications électroniques exploité entièrement ou principalement pour fournir au public des services de communications électroniques, y compris des capacités nationales et internationales, ou des services de communication au public en ligne ou par voie électronique.

Réseau indépendant : tout réseau de communications électroniques réservé à l'usage d'une ou plusieurs personnes constituant un ou plusieurs groupes fermés d'utilisateurs, en vue d'échanger des communications électroniques au sein du même groupe.

Réseau interne : tout réseau de communications électroniques entièrement établi sur une même propriété, sans emprunter ni le domaine public (y compris hertzien), ni l'espace atmosphérique ni une propriété tierce.

Responsable de traitement : la personne physique ou morale, publique ou privée, ou toute autre autorité publique ou tout autre organisme qui, seul on conjointement avec d'autres, détermine les finalités et les moyens d'un traitement de données à caractère personnel. Lorsque des dispositions législatives ou réglementaires déterminent les finalités et moyens d'un traitement, celles-ci peuvent également désigner le responsable de traitement ou fixer les critères permettant de le désigner.

Ressources de numérotation : les préfixes, numéros de téléphone, blocs de numéros de téléphone et codes utilisés pour l'acheminement des communications électroniques qui ne relèvent pas du système de l'adressage de l'Internet.

Service à valeur ajoutée : tout service de communications électroniques qui, n'étant pas un service de diffusion et utilisant des services supports ou les services de communications électroniques, ajoute d'autres services au service support ou répond à de nouveaux besoins spécifiques de communication.

Service d'accès à Internet : un service de communications électroniques accessible au public qui fournit un accès à l'Internet et, partant, une connectivité entre la quasi-totalité des points terminaux de l'Internet, quels que soient la technologie de réseau de communications électroniques ou les équipements terminaux utilisés.

Service de communications électroniques : le service fourni normalement contre rémunération via des réseaux de communications électroniques qui peut comprendre les services téléphoniques, les services d'accès à Internet et les services consistant entièrement ou principalement en la transmission de signaux tels que les services de transmission utilisés pour la fourniture de services de machine à machine et pour la radiodiffusion. Ne sont pas visés les services consistant à fournir des contenus transmis à l'aide de réseaux et de services de communications électroniques ou à exercer une responsabilité éditoriale sur ces contenus.

Service de confiance : un service électronique, qui consiste en la création, la vérification, la validation ou la conservation de signatures électroniques, de cachets électroniques, de certificats électroniques, d'horodatages ou de recommandés électroniques.

Service de confiance qualifié : un service de confiance fourni par un prestataire de services de confiance qualifié.

Service d'envoi recommandé électronique : un service qui permet de transmettre des données entre des tiers par voie électronique, qui fournit des preuves concernant le traitement des données transmises, y compris la preuve de leur envoi et de leur réception, et qui protège les données transmises contre les risques de perte, de vol, d'altération ou de toute modification non autorisée.

Service d'envoi recommandé électronique qualifié : un service d'envoi recommandé électronique qui satisfait aux exigences fixées à l'Article 474.

Service de la société de l'information : tout service réalisé normalement contre rémunération, à distance, par voie électronique et à la demande individuelle d'un destinataire de services.

Service de radiocommunication : tout service impliquant la transmission, l'émission ou la réception d'ondes radioélectriques à des fins spécifiques de communications électroniques.

Service de radiodiffusion : tout service de communications électroniques par voie électronique destiné à être reçu simultanément par l'ensemble du public ou par une catégorie de public et dont le programme principal est composé d'une suite ordonnée d'émissions comportant des images et/ou des sons.

Service téléphonique : service de communications électronique accessible au public permettant d'émettre et de recevoir, directement ou indirectement, des appels

nationaux ou nationaux et internationaux, en composant un ou plusieurs numéros du plan national ou international de numérotation téléphonique.

Service universel : offre minimale de services de communications électroniques à un prix abordable et ce dans le respect des principes d'égalité, de continuité et d'universalité.

Signataire : une personne physique qui crée une signature électronique.

Signature électronique : des données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique et que le signataire utilise pour signer.

Signature électronique avancée : une signature électronique qui satisfait aux exigences fixées à l'Article 427.

Signature électronique qualifiée : une signature électronique qui satisfait aux exigences fixées à l'Article 428 .

Sous-traitant : toute personne physique ou morale, publique ou privée, toute autre autorité publique ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable de traitement.

Spectre radioélectrique : ensemble des ondes radioélectriques dont la fréquence est comprise entre 3 kHz et 3 000 GHz.

Station radioélectrique : un ou plusieurs émetteurs ou récepteurs, ou un ensemble d'émetteurs et de récepteurs y compris les appareils accessoires, nécessaires pour assurer un service de radiocommunication à un emplacement donné.

Système informatique : tout dispositif électronique, magnétique, optique, électrochimique ou tout autre dispositif de haut débit isolé ou interconnecté qui performe la fonction de stockage de données ou l'installation de communications. Ces communications sont directement liées à ou fonctionnent en association avec d'autre(s) dispositif(s).

Système national de données de santé : système national permettant la collecte, le stockage, la mise à disposition et l'utilisation des données de santé des patients définies à l'Article 738, et pour les finalités énumérées à l'Article 739 .

Télémédecine : pratique médicale à distance utilisant les technologies de l'information et de la communication, permettant de mettre en rapport un ou plusieurs professionnels médicaux entre eux ou avec le patient et, le cas échéant, avec d'autres professionnels apportant leurs soins au patient.

Téléservice : tout système d'information ou logiciel permettant aux usagers de procéder par voie électronique à des démarches ou formalités administratives. Il comprend les

traitements automatisés permettant aux usagers (i) d'effectuer, à leur initiative et quelle que soit leur situation géographique, des démarches administratives dématérialisées de toute nature ; (ii) d'y joindre, le cas échéant, des pièces justificatives et ; (iii) au choix des services et des établissements concernés, d'obtenir une réponse de l'administration par voie électronique.

Télésoin : pratique de soins à distance utilisant les technologies de l'information et de la communication, et permettant de mettre en rapport un patient avec un ou plusieurs pharmaciens, auxiliaires médicaux ou professionnels de santé dans l'exercice de leurs compétences.

Traitement de données à caractère personnel ou traitement : toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, que ce procédé soit automatisé ou non, et notamment la collecte, l'enregistrement, l'organisation, la conservation, la structuration, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction.

Titre d'accès : tout billet, document, message ou code, quels qu'en soit la forme et le support, attestant de l'obtention auprès du producteur, de l'organisateur ou du propriétaire des droits d'exploitation du droit d'assister à la manifestation ou au spectacle.

Transmission : tout transfert de données par téléphone, télécopie, courriel ou transfert de fichiers.

Utilisateur : toute personne physique ou morale qui utilise ou demande à bénéficier d'un réseau et/ou d'un service de communications électroniques.

Utilisateur final : utilisateur qui ne fournit pas de réseaux de communications électroniques ouverts au public ou de services de communications électroniques.

Validation : le processus de vérification et de confirmation de la validité d'une signature électronique.

Livre Premier : Protection des données à caractère personnel

Titre 1 : Dispositions générales

Chapitre unique : Dispositions préliminaires

Article 2 Objet

Le présent livre a pour objet de réglementer la collecte, la transmission, le stockage, l'usage et toute autre forme de traitement des données à caractère personnel en vue d'assurer la protection des libertés et droits fondamentaux des personnes physiques et en particulier de la vie privée des personnes concernées.

Ce livre vise à garantir que le traitement de données à caractère personnel, sous quelque forme que ce soit, ne porte atteinte aux libertés et droits fondamentaux des personnes physiques, en prenant en compte les prérogatives de l'État et les intérêts et nécessités du service public, ainsi que les intérêts des entreprises et de la société civile.

Article 3 Champ d'application matériel

Le présent livre s'applique aux traitements automatisés en tout ou partie dedonnées à caractère personnel, ainsi qu'aux traitements non automatisés dedonnées à caractère personnel contenues ou appelées à figurer dans des fichiers,réalisés par l'État, une collectivité locale, une personne morale de droit publicou de droit privé, ou une personne physique.

Article 4 Champ d'application territorial

Le présent livre s'applique aux traitements de données à caractère personnel :

1) réalisés dans le cadre des activités d'un responsable de traitement ou d'un sous-traitant sur le territoire de la République de Djibouti, que le traitement ait lieu ou non en République de Djibouti ;

2) relatifs à des personnes concernées qui se trouvent sur le territoire de la République de Djibouti, par un responsable de traitement ou un sous-traitant qui n'y est pas établi, lorsque les activités de traitement sont liées :

    a) à l'offre de biens ou de services destinée aux personnes concernées en République de Djibouti, qu'un paiement soit exigé ou non desdites personnes ; ou

    b) au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu en République de Djibouti.

3) dont le responsable de traitement ou le sous-traitant n'est pas établi en République de Djibouti mais dans un lieu où le droit de la République de Djibouti s'applique en vertu du droit international public.

Pour les traitements mentionnés au 2), le responsable de traitement désigne à la Commission par écrit un représentant établi sur le territoire de la République de Djibouti qui se substitue à lui dans l'accomplissement des obligations prévues par le présent livre. Cette désignation ne fait pas obstacle aux actions qui pourraient être introduites contre lui.

Article 5 Exclusions

Le présent livre ne s'applique pas :

1) aux traitements de données à caractère personnel mis en œuvre par une personne physique pour l'exercice d'activités exclusivement domestiques ou personnelles à condition que les données ne soient pas destinées à une communication à des tiers ou à la diffusion ;

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

Titre 2 : Droits et obligations des intéressés

Chapitre premier : Obligations des responsables de traitement et de leurs sous-traitants

Article 6 Responsabilité du responsable de traitement pour les traitements effectués sous son autorité

Le responsable de traitement est responsable du respect de l'Article 54. À cet effet, il met en œuvre les mesures techniques et organisationnelles et politiques internes en matière de protection des données à caractère personnel requises pour s'assurer et être en mesure de démontrer que les traitements effectués sous son autorité sont effectués conformément aux dispositions du présent livre.

Le responsable de traitement informe les personnes agissant sous son autorité des dispositions du présent livre ainsi que de toute prescription pertinente relative à la protection de la vie privée et à la protection des données à caractère personnel.

Les données à caractère personnel 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 de traitement ou de celle du sous-traitant, que sur instruction du responsable de traitement, sauf en cas d'obligation légale contraire. Le responsable de traitement demeure responsable pour les opérations de traitement effectuées sur ses instructions.

Toute personne traitant des données à caractère personnel pour le compte du responsable de traitement est considérée comme un sous-traitant au sens du présent livre. Si un sous-traitant détermine les finalités et les moyens d'un traitement, il sera considéré comme un responsable de traitement pour ce qui concerne ce traitement.

Article 7 Responsables conjoints du traitement

Lorsque deux responsables de traitement ou plus déterminent conjointement les finalités et les moyens du traitement, ils sont les responsables conjoints du traitement. Les responsables conjoints d'un traitement définissent de manière transparente leurs obligations respectives aux fins d'assurer le respect des exigences du présent livre, notamment en ce qui concerne l'exercice des droits de la personne concernée et leurs obligations respectives quant à la communication aux personnes concernées des informations prévues par les Article 27,Article 29 et Article 30, par contrat, sauf si, et dans la mesure où, leurs obligations respectives sont définies par la loi à laquelle ils sont soumis.

Le contrat entre les responsables conjoints du traitement reflète dûment leurs rôles respectifs et leurs relations vis-à-vis des personnes concernées. Les principales dispositions du contrat sont mises à la disposition de la personne concernée. Le contrat désigne un point de contact pour les personnes concernées, mais, indépendamment des termes du contrat et de l'existence et de l'identité de ce point de contact, la personne concernée peut exercer indifféremment les droits que lui confère le présent livre à l'égard de chacun des responsables conjoints du traitement.

Article 8 Recours à la sous-traitance

Lorsque le traitement est confié à un sous-traitant, le responsable de traitement doit choisir un sous-traitant présentant des garanties suffisantes au regard de la mise en œuvre des mesures techniques et organisationnelles requises pour assurer que le traitement réponde aux exigences du présent livre et garantisse la protection des droits des personnes concernées, en particulier s'agissant de la confidentialité et de la sécurité des données. Cette exigence ne décharge pas le responsable de traitement de son obligation de veiller au respect de ces mesures.

Le traitement de données à caractère personnel par un sous-traitant est régi par un contrat qui lie le sous-traitant à l'égard du responsable de traitement, définit l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère

personnel et les catégories de personnes concernées, et les obligations et les droits du responsable de traitement. Ce contrat prévoit, notamment, que le sous-traitant :

1) ne traite les données à caractère personnel que sur instruction documentée du responsable de traitement, y compris en ce qui concerne les transferts de données à caractère personnel vers un pays tiers, une société étrangère ou à une organisation internationale, à moins qu'il ne soit tenu d'y procéder en vertu de la loi, auquel cas le sous-traitant informe le responsable de traitement de cette obligation légale avant le traitement, sauf si la loi interdit une telle information pour des motifs d'intérêt public ;

2) veille à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité ;

3) prend toutes les mesures requises en matière de sécurité prévues par le présent chapitre ;

4) respecte les conditions prévues par le présent article et l'Article 9 pour recruter un autre sous-traitant ;

5) tient compte de la nature du traitement, aide le responsable de traitement, par des mesures techniques et organisationnelles appropriées, dans toute la mesure du possible, à s'acquitter de son obligation de donner suite aux demandes dont les personnes concernées le saisissent en vue d'exercer leurs droits prévus au Chapitre 2 : Droit des personnes concernées du Titre 2 du Livre Premier;

6) aide le responsable de traitement à garantir le respect des obligations de confidentialité et de sécurité prévues par le présent chapitre, compte tenu de la nature du traitement et des informations à la disposition du sous-traitant ;

7) selon le choix du responsable de traitement, supprime toutes les données à caractère personnel ou les renvoie au responsable de traitement au terme de la prestation de services relatifs au traitement, et détruit les copies existantes, à moins que la loi n'exige la conservation des données à caractère personnel ; et

8) met à la disposition du responsable de traitement toutes les informations nécessaires pour démontrer le respect des obligations prévues au présent article et pour permettre la réalisation d'audits, y compris des inspections, par le responsable de traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits.

Le contrat liant le sous-traitant au responsable de traitement se présente sous une forme écrite, y compris en format électronique.

Article 9 Chaîne de sous-traitance

Le sous-traitant ne recrute pas un autre sous-traitant sans l'autorisation écrite préalable, spécifique ou générale, du responsable de traitement.

Si une autorisation générale a été donnée au sous-traitant, celui-ci informe le responsable de traitement de tout changement prévu concernant l'ajout ou le remplacement d'autres sous-traitants, afin que le responsable de traitement puisse s'opposer à ces changements.

Lorsqu'un sous-traitant recrute un autre sous-traitant pour mener des activités de traitement spécifiques pour le compte du responsable de traitement, les mêmes obligations en matière de protection de données à caractère personnel que celles fixées dans le contrat entre le responsable de traitement et le sous-traitant sont imposées à cet autre sous-traitant par contrat, en particulier pour ce qui est de présenter des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles requises pour assurer que le traitement réponde aux exigences du présent livre et garantisse la protection des droits des personnes concernées, notamment s'agissant de la confidentialité et de la sécurité des données. Lorsque cet autre sous-traitant ne remplit pas ses obligations en matière de protection des données à caractère personnel, le sous-traitant initial demeure pleinement responsable devant le responsable de traitement de l'exécution par l'autre sous-traitant de ses obligations.

Article 10 Désignation d'un représentant

Lorsqu'un responsable de traitement ou un sous-traitant n'est pas établi sur le territoire de la République de Djibouti, le responsable de traitement ou le sous-traitant y désigne par écrit un représentant, sauf :

1) s'il s'agit d'un traitement qui est occasionnel, qui n'implique pas un traitement à grande échelle des catégories particulières de données visées à l'Article 62 , ou un traitement de données à caractère personnel relatives aux infractions, condamnations pénales et mesures de sûreté visées à l'Article 63, et qui n'est pas susceptible d'engendrer un risque pour les droits et libertés des personnes concernées, compte tenu de la nature, du contexte, de la portée et des finalités du traitement ; ou

2) pour les traitements effectués par une autorité publique.

Le représentant est mandaté pour être la personne à qui la Commission et les personnes concernées doivent s'adresser, en plus ou à la place du responsable de traitement ou du sous-traitant, pour toutes les questions relatives au traitement, aux fins d'assurer le respect du présent livre.

La désignation d'un représentant ne fait pas obstacle l'initiation d'actions en justice qui pourraient être intentées contre le responsable de traitement ou le sous-traitant lui-même pour violation des dispositions du présent livre.

Article 11 Protection des données à caractère personnel dès la conception et protection des données par défaut

Au regard de la nature des données à caractère personnel et des risques présentés par le traitement pour les droits et libertés des personnes concernées, le responsable de traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données rappelés à l'Article 54 de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent livre et de protéger les droits des personnes concernées.

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

Article 12 Confidentialité

Le traitement des données à caractère personnel est confidentiel. Il est effectué par des personnes qui agissent sous l'autorité du responsable de traitement et seulement sur ses instructions.

Pour la réalisation du traitement, le responsable de traitement 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.

Le responsable de traitement doit veiller à ce que les personnes ayant accès aux données soient tenues par une obligation légale, statutaire ou contractuelle au respect du caractère confidentiel des données à caractère personnel.

Article 13 Sécurité

Le responsable de traitement et le sous-traitant prennent les mesures nécessaires afin de garantir que toute personne agissant sous l'autorité du responsable de traitement ou celle

du sous-traitant, qui a accès à des données à caractère personnel, ne les traite que sur instruction du responsable de traitement.

Le responsable de traitement et le sous-traitant prennent toute précaution utile, au regard de la nature des données à caractère personnel et des risques présentés par le traitement pour les droits et libertés des personnes concernées, pour préserver la sécurité des données et les droits et libertés des personnes concernées, et, notamment, empêcher que les données soient altérées, endommagées, détruites, perdues ou que des tiers non autorisés y aient accès ou que celles-ci soient divulguées de manière non-autorisée. Ils prennent, en particulier, toute mesure technique et organisationnelle visant à :

1) garantir que, pour l'utilisation d'un système de traitement automatisé des données, les personnes autorisées ne puissent accéder qu'aux données à caractère personnel relevant de leur compétence et de leur habilitation et que leur accès soit limité à ce dont elles ont besoin pour l'exercice de leurs fonctions ou ce qui est nécessaire pour les nécessités du service ;

2) garantir que puisse être vérifiée et constatée l'identité des tiers auxquels des données à caractère personnel peuvent être transmises ;

3) garantir que puisse être vérifiée et constatée a posteriori l'identité des personnes ayant eu accès au système de traitement automatisé des données et quelles données ont été lues ou introduites dans le système, à quel moment et par quelle personne ;

4) empêcher toute personne non autorisée d'accéder aux locaux et aux équipements utilisés pour le traitement des données à caractère personnel ;

5) empêcher que des supports de données à caractère personnel puissent être lus, copiés, modifiés, détruits ou déplacés par une personne non autorisée ;

6) empêcher l'introduction non autorisée de toute donnée dans le système de traitement automatisé des données ainsi que toute prise de connaissance, toute modification ou tout effacement non autorisés des données à caractère personnel enregistrées ;

7) empêcher que des systèmes de traitement automatisé des données puissent être utilisés par des personnes non autorisées à l'aide d'installations de transmission de données ;

8) empêcher que, lors de la communication des données à caractère personnel et du transport des supports de ces données, les données puissent être lues, copiées, modifiées ou effacées de façon non autorisée ;

9) sauvegarder les données à caractère personnel par la constitution de copies de sécurité ;

10) rafraîchir et si nécessaire, convertir les données à caractère personnel pour un stockage pérenne ;

11) rendre les données à caractère personnel inexploitables pour toute personne qui n'est pas autorisée à y avoir accès ;

12) rendre impossible la réidentification des personnes concernées.

Ces mesures peuvent notamment comprendre la pseudonymisation et le chiffrement des données à caractère personnel, ainsi que des procédures visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles mise en œuvre pour assurer la sécurité des traitements.

Les décrets portant création des traitements de certaines catégories de données à caractère personnel conformément à l'Article 70 peuvent fixer des prescriptions techniques additionnelles spécifiques auxquelles les traitements qu'ils instituent doivent être conformes.

Article 14 Notification des atteintes à la sécurité de données à caractère personnel à la Commission

En cas d'atteinte à la sécurité de données à caractère personnel, le responsable de traitement notifie la Commission, dans les meilleurs délais et, au plus tard soixante-douze (72) heures après en avoir pris connaissance. Lorsque la notification à la Commission n'a pas lieu dans les soixante-douze (72) heures, elle est accompagnée des motifs du retard.

Est notamment considérée comme une atteinte à la sécurité de données à caractère personnel tout atteinte entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation ou l'accès non autorisé à des données à caractère personnel faisant l'objet d'un traitement.

Le sous-traitant notifie au responsable de traitement toute atteinte à la sécurité de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance.

Les notifications visées au premier et au troisième alinéa du présent article décrivent et indiquent :

1) la nature de l'atteinte à la sécurité des données à caractère personnel y compris les catégories et le nombre approximatif de personnes concernées par l'atteinte et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;

2) le nom et les coordonnées du délégué à la protection des données, du représentant du responsable de traitement ou du sous-traitant ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;

3) les conséquences probables de l'atteinte à la sécurité des données à caractère personnel ;

4) les mesures prises ou que le responsable de traitement ou le sous-traitant propose de prendre pour remédier à l'atteinte à la sécurité des données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Si, et dans la mesure où, il n'est pas possible de fournir toutes les informations en même temps, les informations peuvent être communiquées de manière échelonnée sans autre retard indu.

Le responsable de traitement documente dans un registre toute atteinte à la sécurité de données à caractère personnel, en indiquant les faits concernant les atteintes, leurs effets et les mesures prises pour y remédier. La documentation ainsi constituée est communiquée sur demande à la Commission pour lui permettre de vérifier le respect du présent article.

Article 15 Notification des atteintes à la sécurité de données à caractère personnel à la personne concernée

Lorsqu'une atteinte à la sécurité de données à caractère personnel visée à l'Article 14 est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne concernée, le responsable de traitement informe la personne concernée de cette atteinte dans les meilleurs délais.

L'information à la personne concernée décrit, en des termes clairs et simples, la nature de l'atteinte à la sécurité de données à caractère personnel et inclut les informations prévues au 2), 3) et 4) de l'Article 14.

L'information à la personne concernée n'est pas nécessaire si l'une ou l'autre des conditions suivantes est remplie :

1) le responsable de traitement a mis en œuvre les mesures de protection techniques et organisationnelles appropriées et ces mesures ont été appliquées aux données à caractère personnel affectées par l'atteinte, en particulier les mesures qui rendent les données à caractère personnel incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès, telles que le chiffrement ;

2) le responsable de traitement a pris des mesures ultérieures qui garantissent que le risque élevé pour les droits et libertés des personnes concernées n'est plus susceptible de se matérialiser ;

3) elle exigerait des efforts disproportionnés. Dans ce cas, il est plutôt procédé à une communication publique ou à une mesure similaire permettant aux personnes concernées d'être informées de manière tout aussi efficace.

Si le responsable de traitement n'a pas déjà informé la personne concernée de l'atteinte à la sécurité de données à caractère personnel la concernant, la Commission peut, après avoir examiné si cette atteinte est susceptible d'engendrer un risque élevé, exiger du responsable de traitement qu'il procède à cette information, sauf si elle considère que l'une ou l'autre des conditions rendant l'information non nécessaire est remplie.

Article 16 Conservation

Les données à caractère personnel ne peuvent être conservées au-delà de la durée prévue au 5) de l'Article 54 qu'en vue d'être traitées à des fins historiques, statistiques ou scientifiques et dans les conditions prévues par la loi.

Il peut être procédé à un traitement ayant des finalités autres que celles mentionnées au premier alinéa :

1) soit avec l'accord exprès de la personne concernée ;

2) soit avec l'autorisation de la Commission ;

3) soit dans les conditions prévues à l'avant-dernier alinéa de l'Article 62 de la Section 1 : Traitements de données à caractère personnel réalisés aux fins de recherche, d'étude ou d'évaluation dans le domaine de la santé du Chapitre 3 du Titre 3 du Livre Premier s'agissant des catégories de données concernées par ces articles.

Article 17 Pérennité

Le responsable de traitement est tenu de prendre toute mesure utile pour assurer que les données à caractère personnel pourront être exploitées quel que soit le support technique utilisé. Il s'assure que l'évolution de la technologie ne sera pas un obstacle à cette exploitation.

Article 18 Coopération avec la Commission

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

Les responsables de traitement et les sous-traitants ne peuvent s'opposer à l'action de la Commission ou de ses agents et doivent prendre toutes mesures utiles afin de faciliter sa tâche.

Chapitre 2 : Droit des personnes concernées

Section préliminaire : Dispositions générales

Article 19 Forme des demandes

Les demandes présentées par les personnes concernées exerçant les droits qui leur sont conférés par les dispositions du présent chapitre sont transmise au responsable de traitement par écrit et quel que soit le support, y compris par voie électronique lorsque cela est possible.

Article 20 Confirmation de l'identité de la personne présentant la demande

Lorsque le responsable de traitement a des doutes raisonnables quant à l'identité de la personne présentant une demande en application des dispositions du présent chapitre, il peut demander que lui soient fournies des informations supplémentaires pour confirmer l'identité de la personne concernée.

Article 21 Traitements ne nécessitant pas l'identification de la personne concernée

Si les finalités pour lesquelles des données à caractère personnel sont traitées n'imposent pas ou n'imposent plus au responsable de traitement d'identifier une personne concernée, celui-ci n'est pas tenu de conserver, d'obtenir ou de traiter des informations supplémentaires pour identifier la personne concernée à la seule fin de respecter les dispositions du présent livre.

Lorsque, dans ce cas, le responsable de traitement est à même de démontrer qu'il n'est pas en mesure d'identifier la personne concernée, il en informe la personne concernée, si possible, et les dispositions des Section 2 : Droit d'accès, Section 4 : Droit de rectification, Section 5 : Droit à l'effacement et Section 6 : Droit à la portabilité du présent chapitre ne sont pas applicables, sauf lorsque la personne concernée fournit, aux fins d'exercer les droits que lui confèrent ces dispositions, des informations complémentaires qui permettent de l'identifier.

Article 22 Gratuité de l'exercice des droits de la personne concernée

Hors les cas prévus par les dispositions du présent chapitre, aucun paiement ne peut être exigé par le responsable de traitement pour fournir les informations, communiquer les documents requis, mettre en œuvre les droits des personnes concernées prévus par le présent chapitre et faire droit aux demandes présentées par les personnes concernées.

Lorsque les demandes d'une personne concernée sont manifestement infondées ou excessives, notamment en raison de leur caractère répétitif, le responsable de 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, ou refuser de donner suite à ces demandes. La charge de la preuve du caractère manifestement infondé ou excessif de la demande incombe au responsable de traitement.

Article 23 Transparence des informations communiquées à la personne concernée

Le responsable de traitement prend les mesures appropriées pour fournir toute information et communiquer tout document requis par les dispositions du Chapitre 2 : Droit des personnes concernées du présent titre à la personne concernée d'une façon concise, transparente, compréhensible et aisément accessible et en des termes clairs et simples, en particulier pour toute information destinée spécifiquement à un mineur. Les informations sont fournies par écrit, y compris, lorsque c'est approprié et avec l'accord de la personne concernée, par voie électronique. Lorsque la personne concernée en fait la demande, les informations peuvent être fournies oralement, à condition qu'elle soit en mesure de démontrer son identité au responsable de traitement.

Article 24 Facilitation de l'exercice de leurs droits par les personnes concernées et obligation de faire droit aux demandes

Le responsable de traitement prend les mesures nécessaires pour faciliter l'exercice par les personnes concernées des droits qui leur sont conférés par les dispositions du présent chapitre.

Le responsable de traitement est tenu de faire droit aux demandes présentées par les personnes concernées exerçant ces droits dans les limites prévues par les dispositions du Chapitre 2 : Droit des personnes concernées du présent titre. Le responsable de traitement doit notamment faire toute diligence pour tenir les données à caractère personnel à jour, pour rectifier ou supprimer les données inexactes, incomplètes, ou non pertinentes, ainsi que celles obtenues ou traitées en méconnaissance des dispositions du Chapitre Premier du Titre 3 du présent livre. Dans les cas visés à l'Article 21 le responsable de traitement ne peut refuser de donner suite à la demande de la personne concernée à moins qu'il ne démontre qu'il n'est pas en mesure d'identifier la personne concernée.

Article 25 Information sur les mesures prises et droit de recours

Le responsable de traitement informe la personne concernée des mesures prises à la suite d'une demande formulée en application des dispositions du Chapitre 2 du présent titre dans les meilleurs délais et en tout état de cause dans un délai d'un (01) mois à compter de la réception de la demande. Au besoin, ce délai peut être prolongé de deux mois

compte tenu de la complexité et du nombre de demandes reçues. Le responsable de traitement informe la personne concernée de cette prolongation et des motifs avant l'expiration du délai d'un mois précité. Lorsque la personne concernée présente sa demande sous une forme électronique, les informations sont fournies par voie électronique, à moins que la personne concernée ne demande qu'il en soit autrement.

Si le responsable de traitement n'entend pas donner pas suite à la demande formulée par la personne concernée, il informe celle-ci sans tarder et au plus tard dans le délai d'un (1) mois précité des motifs de son inaction ou son refus et de la possibilité d'introduire une réclamation auprès de la Commission et de former un recours juridictionnel.

Article 26 Droit d'introduire une réclamation auprès de la Commission

En cas de contestation des mesures prises par le responsable de traitement ou de refus du responsable de traitement de faire droit aux demandes présentées par une personne concernée ou de non-respect des délais prévus par les dispositions du présent chapitre, la personne concernée peut adresser une plainte à la Commission.

Sans préjudice de tout autre recours administratif ou juridictionnel, toute personne concernée a le droit d'introduire une réclamation auprès de la Commission si elle considère que le traitement de données à caractère personnel la concernant constitue une violation des dispositions du présent livre. La Commission informe la personne concernée de l'état d'avancement de la réclamation et des suites qui y sont données, y compris de la possibilité d'introduire un recours juridictionnel. À défaut d'information ou de suite donnée par la Commission dans un délai de deux (2) mois à compter de la réclamation, la personne concernée peut saisir le Tribunal Administratif de Première Instance afin d'enjoindre la Commission à l'informer de l'état d'avancement de la réclamation.

Section 1 : Droit à l'information

Article 27 Informations à communiquer par le responsable de traitement lors de la collecte

Lorsque des données à caractère personnel relatives à une personne concernée sont collectées auprès de cette personne, le responsable de traitement ou son représentant lui fournit, au plus tard lors de la collecte et quels que soient les moyens et supports employés, les informations suivantes :

1) son identité et ses coordonnées et, le cas échéant, celles de son représentant ;

2) le cas échéant, les coordonnées du délégué à la protection des données ;

3) la ou les finalités déterminées poursuivies par le traitement auquel les données à caractère personnel sont destinées ainsi que la base juridique établissant la licéité du traitement conformément à l'Article 55 ;

4) lorsque le traitement est fondé sur des intérêts légitimes poursuivis par le responsable de traitement ou par un destinataire/tiers conformément au 6) de l'Article 55 , les intérêts légitimes dont il est question ;

5) les catégories de personnes ayant accès aux données à caractère personnel collectées ;

6) les destinataires ou les catégories de destinataires des données à caractère personnel auxquels celles-ci sont susceptibles d'être communiquées, s'ils existent ;

7) le cas échéant, le fait que le responsable de traitement a l'intention d'effectuer un transfert des données à caractère personnel vers un pays tiers, une société étrangère ou à une organisation internationale ;

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

9) l'existence des autres droits dont jouit la personne concernée en cette qualité conformément au présent Chapitre : droit de demander au responsable de traitement l'accès aux données à caractère personnel, leur rectification ou effacement, droit de s'opposer au traitement et droit à la portabilité des données ;

10) lorsque le traitement est fondé sur le consentement de la personne concernée conformément au 1) de l'Article 55, l'existence du droit de retirer son consentement à tout moment, sans porter atteinte à la licéité du traitement fondé sur le consentement effectué avant le retrait de celui-ci ;

11) le droit d'introduire une réclamation auprès de la Commission et les coordonnées de la Commission ;

12) du caractère obligatoire ou facultatif des réponses, en particulier des informations sur la question de savoir si l'exigence de fourniture de données à caractère personnel a un caractère légal ou contractuel ou si elle conditionne la conclusion d'un contrat et si la personne concernée est tenue de fournir les données à caractère personnel, ainsi que sur les conséquences éventuelles de la non-fourniture de ces données ;

13) l'existence d'une prise de décision automatisée conformément à l'Article 65 et, dans ce cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée.

Lorsque des données à caractère personnel sont recueillies par voie de questionnaires écrits, ceux-ci doivent porter mention des prescriptions du présent article.

Lorsqu'il a l'intention d'effectuer un traitement ultérieur des données à caractère personnel pour une finalité autre que celle pour laquelle les données à caractère personnel ont été collectées, le responsable de traitement fournit au préalable à la personne concernée des informations au sujet de cette autre finalité et toute autre information pertinente visée au présent article.

Le présent article ne s'applique pas lorsque, et dans la mesure où, la personne concernée dispose déjà de ces informations.

Article 28 Information relative au droit d'opposition

Lorsque des données à caractère personnel sont recueillies par voie de questionnaires écrits, ceux-ci doivent comporter une mention spécifique demandant à la personne concernée si elle souhaite exercer son droit d'opposition.

Lorsque les données à caractère personnel sont collectées auprès de la personne concernée autrement que par écrit, le responsable de traitement demande à celle-ci si elle souhaite exercer le droit d'opposition, soit sur un document qu'il lui communique à cette fin au plus tard deux mois après la collecte des données à caractère personnel, soit par tout moyen technique qui permet de conserver la preuve que la personne concernée a eu la possibilité d'exercer son droit.

Article 29 Informations spécifiques à communiquer aux utilisateurs de réseaux de communications électroniques

Toute personne utilisatrice d'un service de communications électroniques doit être informée de manière claire et complète, sauf si elle l'a été au préalable, par le responsable de traitement ou son représentant :

1) de la finalité de toute action tendant à accéder, par voie de transmission électronique, à des informations déjà stockées dans son équipement terminal, ou à inscrire des informations dans cet équipement ; et

2) des moyens dont elle dispose pour s'y opposer.

Ces accès ou inscriptions ne peuvent avoir lieu qu'à condition que 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 la personne utilisatrice ou l'inscription d'informations dans l'équipement terminal de la personne utilisatrice :

1) soit a pour finalité exclusive de permettre ou faciliter la communication par voie électronique ;

2) soit est strictement nécessaire à la fourniture d'un service de communication au public en ligne à la demande expresse de la personne utilisatrice.

Article 30 Informations à communiquer par le responsable de traitement en cas de collecte indirecte

Lorsque les données à caractère personnel n'ont pas été collectées auprès de la personne concernée, le responsable de traitement ou son représentant fournit à cette dernière les informations énumérées à l'Article 27 ainsi que les informations suivantes :

1) les catégories de données à caractère personnel concernées ; et

2) la source d'où proviennent les données à caractère personnel et, le cas échéant, une mention indiquant qu'elles sont issues ou non de sources accessibles au public.

Ces informations sont communiquées :

1) dans un délai raisonnable ne dépassant pas un mois après avoir obtenu les données à caractère personnel, au regard des circonstances particulières dans lesquelles les données à caractère personnel sont traitées ;

2) si les données à caractère personnel doivent être utilisées aux fins de la communication avec la personne concernée, au plus tard au moment de la première communication à celle-ci ; ou

3) s'il est envisagé de communiquer les informations à un autre destinataire avant que les données à caractère personnel ne soient communiquées pour la première fois.

Lorsqu'il a l'intention d'effectuer un traitement ultérieur des données à caractère personnel pour une finalité autre que celle pour laquelle les données à caractère personnel ont été obtenues, le responsable de traitement fournit au préalable à la personne concernée des informations au sujet de cette autre finalité et toute autre information pertinente visée au présent article.

Le présent article ne s'applique pas lorsque, et dans la mesure où :

1) la personne concernée dispose déjà de ces informations ;

2) la fourniture de ces informations se révèle impossible ou exigerait des efforts disproportionnés par rapport aux objectifs du traitement, en particulier pour les traitements nécessaires à la conservation de ces données à des fins historiques,

statistiques ou scientifiques ou à la réutilisation de ces données à des fins statistiques dans les conditions prévues par la loi ; ou

3) l'obtention ou la communication des données à caractère personnel sont effectués en application d'une disposition légale ou réglementaire s'imposant au responsable de traitement.

Article 31 Limites au droit à l'information

Si les données à caractère personnel collectées sont appelées à faire l'objet à bref délai d'un procédé d'anonymisation préalablement reconnu conforme aux dispositions du présent Livre par la Commission, les informations délivrées par le responsable de traitement à la personne concernée peuvent se limiter à celles mentionnées au 1), 2) et 3) de l'Article 27.

Les dispositions de la présente section ne s'appliquent pas :

1) aux données à caractère personnel collectées dans les conditions prévues à l'Article 30 et utilisées dans le cadre d'un traitement mis en œuvre pour le compte de l'État et intéressant la sûreté de l'État, la défense, la sécurité publique ou ayant pour objet l'exécution de condamnations pénales ou de mesures de sûreté, dans la mesure où une telle limitation est nécessaire au respect des fins poursuivies par le traitement ; et

2) aux traitements de données à caractère personnel ayant pour objet la prévention, la recherche, la constatation ou la poursuite d'infractions pénales.

Section 2 : Droit d'accès

Article 32 Périmètre du droit d'accès

Toute personne physique justifiant de son identité a le droit d'interroger le responsable d'un traitement de données à caractère personnel en vue d'obtenir la confirmation que des données à caractère personnel la concernant font ou ne font pas l'objet de ce traitement, et, dans l'affirmative, les informations suivantes :

1) des informations relatives aux finalités du traitement, aux catégories de données à caractère personnel traitées et aux destinataires ou aux catégories de destinataires auxquels les données ont été ou seront communiquées ;

2) le cas échéant, des informations relatives aux transferts de données à caractère personnel envisagés à destination d'un pays tiers, d'une société étrangère ou d'une organisation internationale et des garanties mises en place par le responsable de traitement.

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

4) l'existence des droits dont jouit la personne concernée en cette qualité conformément aux dispositions du présent Chapitre et les modalités selon lesquelles elle peut les exercer : droit de demander au responsable de traitement l'accès aux données à caractère personnel, leur rectification ou effacement, droit de s'opposer au traitement et droit à la portabilité des données et gestion de ces données à son décès ;

5) le droit d'introduire une réclamation auprès de la Commission et les coordonnées de la Commission ;

6) lorsque les données à caractère personnel ne sont pas collectées auprès de la personne concernée, toute information disponible quant à leur source ;

7) l'existence d'une prise de décision automatisée conformément à l'Article 65 et, dans ce 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 33 Droit d'obtenir une copie des données à caractère personnel

Le responsable de traitement délivre une copie des données à caractère personnel à la personne concernée à sa demande, dans un format accessible et sous une forme intelligible. 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 responsable de traitement peut subordonner la délivrance de cette copie au paiement d'une somme qui ne peut excéder le coût de la reproduction.

Le responsable de traitement peut exiger le paiement de frais raisonnables basés sur les coûts administratifs pour toute copie supplémentaire demandée par la personne concernée.

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 la Commission qui procède aux vérifications nécessaires.

Lorsqu'il y a lieu de craindre la dissimulation ou la disparition des données à caractère personnel, la personne concernée ou la Commission peut saisir le juge compétent pour que soient ordonnées toutes mesures de nature à éviter cette dissimulation ou cette disparition.

Article 34 Droit d'accès du patient

Lorsque l'exercice du droit d'accès concerne des données de santé à caractère personnel, le droit d'accès est exercé par la personne concernée elle-même ou par l'intermédiaire d'un médecin de son choix. En cas de décès de la personne concernée, ses ayants droits peuvent exercer, par l'intermédiaire d'un médecin qu'ils désignent, ce droit d'accès.

Article 35 Demandes manifestement abusives

Le responsable de 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 de traitement auprès duquel elles sont adressées.

Article 36 Limites au droit d'accès

Les dispositions de la présente section ne s'appliquent pas lorsque les données à caractère personnel sont conservées sous une forme excluant manifestement tout risque d'atteinte à la vie privée des personnes concernées et pendant une durée n'excédant pas celle nécessaire aux seules finalités d'établissement de statistiques ou de recherche scientifique ou historique.

Les dispositions de la présente section sont applicables aux traitements mis en œuvre par les administrations publiques et les personnes privées chargées d'une mission de service public qui ont pour mission de prévenir, rechercher ou constater des infractions uniquement si un tel droit a été prévu par l'autorisation mentionnée auxArticle 69,Article 70,Article 71 et Article 72.

Lorsque des données de santé à caractère personnel sont traitées aux fins de recherche, d'étude, d'évaluation ou de suivi dans le domaine de la santé conformément aux dispositions de la Section 1 du Chapitre 3 du Titre 3 du présent livre, qu'il est manifeste qu'il n'existe aucun risque qu'il soit porté atteinte à la vie privée de cette personne et que les données ne sont pas utilisées pour prendre des mesures à l'égard d'une personne concernée individuellement, la communication des données peut, dès lors qu'elle serait susceptible de nuire gravement à la recherche, l'étude, l'évaluation ou le suivi poursuivi, être différée au plus tard jusqu'à son achèvement. Dans ce cas, la personne concernée doit avoir préalablement consenti par écrit au traitement des données à caractère personnel la concernant pour ces fins et la communication de ces données peut être différée.

Section 3 : Droit d'opposition

Article 37 Modalités d'exercice du droit d'opposition

Toute personne physique a le droit de s'opposer à tout moment et sans frais, pour des raisons tenant à sa situation particulière, à un traitement de données à caractère

personnel la concernant fondé sur le 5) ou 6) de l'Article 55, y compris à la prise de décision automatisée conformément à l'Article 65 sur ces fondements. En cas d'opposition au traitement, le responsable de traitement cesse de traiter les données à caractère personnel concernées à moins qu'il ne démontre qu'il existe des motifs légitimes et impérieux pour le traitement qui prévalent sur les intérêts et les droits et libertés de la personne concernée, ou pour la constatation, l'exercice ou la défense de droits en justice.

Lorsque les données à caractère personnel sont traitées à des fins de prospection, la personne concernée a le droit de s'opposer à tout moment et sans frais, à ce que les données la concernant soient utilisées à des fins de prospection, notamment commerciale, par le responsable de traitement actuel ou celui d'un traitement ultérieur, y compris pour la prise de décision automatisée conformément à l'Article 65 en lien avec une telle prospection. En cas d'opposition au traitement à des fins de prospection, le responsable de traitement cesse de traiter les données à caractère personnel concernées à ces fins.

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

Sous réserve des dispositions de l'Article 27, le droit d'opposition prévu par le présent article fait l'objet d'une information spécifique et explicite à l'attention de la personne concernée au plus tard lors de la première communication avec celle-ci. Cette information est présentée clairement et séparément de toute autre information.

Les dispositions du premier alinéa ne s'appliquent pas lorsque le traitement répond à une obligation légale ou lorsque l'application de ces dispositions a été écartée par une disposition expresse de l'acte réglementaire autorisant le traitement.

Section 4 : Droit de rectification

Article 38 Modalités d'exercice du droit de rectification

Toute personne physique justifiant de son identité peut exiger d'un responsable de traitement que soient, selon le cas, rectifiées, complétées ou mises à jour les données à caractère personnel la concernant, qui sont inexactes, incomplètes ou, équivoques.

En cas de contestation, la charge de la preuve incombe au responsable auprès duquel est exercé le droit de rectification sauf lorsqu'il est établi que les données à caractère personnel en cause ont été communiquées par l'intéressé ou avec son accord.

Lorsqu'elle obtient une modification de l'enregistrement, la personne concernée est en droit d'obtenir le remboursement des frais correspondant au coût d'accès à la copie des données à caractère personnel la concernant mentionné au deuxième alinéa de l'Article 33.

Le responsable de traitement notifie à chaque destinataire auquel les données à caractère personnel ont été communiquées toute rectification de données à caractère personnel effectuée conformément à la demande reçue. Le responsable de traitement fournit à la personne concernée des informations sur ces destinataires si celle-ci en fait la demande.

Article 39 Limites au droit de rectification

Les dispositions de la présente section sont applicables aux traitements mis en œuvre par les administrations publiques et les personnes privées chargées d'une mission de service public qui ont pour mission de prévenir, rechercher ou constater des infractions uniquement si un tel droit a été prévu par l'autorisation mentionnée auxArticle 70, Article 71 etArticle 72.

Article 40 Fichier nominatif

Sur avis favorable de la Commission, un fichier nominatif peut être complété ou corrigé même d'office lorsque l'organisme qui le tient acquiert connaissance de l'inexactitude ou du caractère incomplet d'une information nominative contenue dans ce fichier.

Si une information a été transmise à un tiers, sa rectification ou son annulation doit être notifiée à ce tiers, sauf dispense accordée par la Commission.

Section 5 : Droit à l'effacement

Article 41 Motifs justifiant une demande d'effacement

La personne concernée a le droit d'obtenir du responsable de traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant, lorsque l'un des motifs suivants s'applique :

1) les données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière ;

2) la personne concernée retire le consentement sur lequel est fondé le traitement conformément au 1) de l'Article 55 ou au 1) de l'Article 62 et il n'existe pas d'autre base juridique fondant le traitement ;

3) la personne concernée s'oppose au traitement en vertu du premier alinéa de l'Article 37 et il n'existe pas de motif légitime et impérieux justifiant le maintien du traitement ;

4) la personne concernée s'oppose au traitement en vertu du deuxième alinéa de l'Article 37 ;

5) la personne concernée s'oppose au traitement en vertu du troisième alinéa de l'Article 37 et le traitement n'est pas nécessaire à l'exécution d'une mission d'intérêt public justifiant son maintien ;

6) les données à caractère personnel font ou ont fait l'objet d'un traitement interdit ou illicite ;

7) les données à caractère personnel doivent être effacées pour respecter une obligation légale à laquelle le responsable de traitement est soumis ;

8) les données à caractère personnel ont été collectées conformément à l'Article 59 dans le cadre de l'offre de services de la société de l'information lorsque la personne était mineure au moment de la collecte.

Article 42 Obligation de mettre en œuvre les demandes d'effacement

Le responsable de traitement a l'obligation d'effacer les données à caractère personnel faisant l'objet de la demande d'effacement au plus tard dans un délai de trente (30) jours. Lorsque l'effacement est effectué, le responsable de traitement ne procède à aucun autre traitement de ces données à caractère personnel.

L'effacement doit être effectué en procédant à une suppression totale des données à caractère personnelle faisant l'objet de la demande d'effacement, y compris toute copie de ces données. Le responsable de traitement ne peut conserver aucune copie des données à caractère personnel faisant l'objet de la demande d'effacement.

Article 43 Mécanismes visant à assurer l'effectivité du droit à l'effacement

Le responsable de traitement notifie chaque destinataire auquel les données à caractère personnel ont été communiquées tout effacement de données à caractère personnel effectué, à moins qu'une telle communication se révèle impossible ou exige des efforts disproportionnés. Le responsable de traitement fournit à la personne concernée des informations sur ces destinataires.

Lorsque le responsable de traitement a rendu publiques les données à caractère personnel objet de la demande d'effacement et qu'il est tenu de les effacer, le responsable de traitement prend toutes les mesures raisonnables, y compris d'ordre technique, pour informer les tiers, les destinataires et les autres responsables de traitement qui traitent ces données à caractère personnel que la personne concernée a demandé leur effacement ainsi que l'effacement par ceux-ci de tout lien vers ces données à caractère personnel, ou de toute copie ou reproduction de celles-ci.

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

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

Article 44 Modalités de mise en œuvre du droit à l'effacement

La Commission adopte des mesures ou des lignes directrices afin de préciser les conditions d'effacement des données à caractère personnel faisant l'objet d'une demande d'effacement, de suppression des liens vers ces données ainsi que des copies ou des reproductions de celles-ci existant dans les services de communications électroniques accessibles au public et dans les services de communication au public en ligne.

Article 45 Limites au droit à l'effacement

Les dispositions de la présente section ne s'appliquent pas dans la mesure où le traitement est nécessaire :

1) à l'exercice du droit à la liberté d'expression et d'information ;

2) pour respecter une obligation qui requiert le traitement prévue par la loi et à laquelle le responsable de traitement est soumis, ou pour exécuter une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable de traitement ;

3) pour des motifs d'intérêt public dans le domaine de la santé publique conformément au 4) ou au 5) de l'Article 62 ;

4) à des fins de recherche scientifique ou historique ou à des fins statistiques dans la mesure où le droit à l'effacement est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs dudit traitement ; ou

5) à la constatation, à l'exercice ou à la défense de droits en justice.

Section 6 : Droit à la portabilité

Article 46 Droit d'obtenir une copie des données dans un format électronique structuré

Les personnes concernées ont le droit de recevoir les données à caractère personnel les concernant qu'elles ont fournies à un responsable de traitement, dans un format

structuré, couramment utilisé et lisible par machine, et ont le droit de transmettre ces données à un autre responsable de traitement sans que le responsable de traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle, lorsque :

1) le traitement est fondé sur le consentement conformément au 1) de l'Article 55 ou au 1) de l'Article 62 ou sur un contrat conformément au 2) de l'Article 55 ; et

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

Article 47 Droit au transfert des données et à leur effacement

Lorsque la personne concernée exerce son droit à la portabilité, elle a le droit d'obtenir que les données à caractère personnel soient transmises directement d'un responsable de traitement à un autre, lorsque cela est techniquement possible.

L'exercice du droit à la portabilité ne fait pas obstacle à l'exercice simultané du droit à l'effacement auprès d'un ou plusieurs responsables de traitement.

Article 48 Limites au droit à la portabilité

Les dispositions de la présente section ne s'appliquent pas aux traitements nécessaires à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable de traitement.

Section 7 : Modalités d'exercice particulières pour les traitements intéressant la sûreté de l'État, la défense ou la sécurité publique

Article 49 Modalités particulières d'accès et de rectification pour les traitements intéressant la sûreté de l'État, la défense ou la sécurité publique

Par dérogation aux dispositions du présent chapitre, lorsque le traitement intéresse la sûreté de l'État, la défense ou la sécurité publique, les droit d'accès et de rectification s'exercent dans les conditions suivantes :

1) la demande est adressée à la Commission qui désigne l'un de ses membres ayant la qualité de magistrat pour mener les investigations utiles et faire procéder aux modifications nécessaires, qui peut se faire assister d'un autre agent de la Commission ;

2) la Commission informe la personne concernée qu'il a été procédé aux vérifications ;

3) lorsque la Commission constate, en accord avec le responsable de traitement, que la communication des données à caractère personnel qui font l'objet du traitement ne met pas en cause ses finalités, la sûreté de l'État, la défense ou la sécurité publique, ces données peuvent être communiquées à la personne ayant fait la demande d'accès ;

4) lorsque le traitement est susceptible de contenir des informations dont la communication ne mettrait pas en cause ses finalités, l'acte réglementaire portant création du traitement peut prévoir que ces informations peuvent être communiquées à la personne ayant fait la demande d'accès par le responsable de traitement directement.

Article 50 Modalités particulières d'accès et de rectification pour les traitements relatifs aux infractions

Les dispositions de l'Article 49 sont applicables aux traitements mis en œuvre par les administrations publiques et les personnes privées chargées d'une mission de service public qui ont pour mission de prévenir, rechercher ou constater des infractions uniquement lorsqu'un tel droit a été prévu par l'autorisation mentionnée auxArticle 69,Article 70, Article 71 et Article 72.

Section 8 : Modalités particulières relatives aux traitements concernant des personnes décédées

Article 51 Information de la personne concernée

Tout prestataire d'un service de communication au public en ligne mettant en œuvre un traitement de données à caractère personnel informe la personne concernée du sort des données qui la concernent à son décès et lui permet de choisir de communiquer ou non ses données à un tiers qu'elle désigne.

Article 52 Gestion des données à caractère personnel suivant les directives de la personne concernée

La personne concernée peut indiquer au responsable de traitement dans des directives la manière dont elle souhaite que soient exercés les droits qui lui sont conférés par les dispositions du présent chapitre à son décès, et en particulier s'agissant de la conservation, de l'effacement ou de la communication des données à caractère personnel la concernant à des tiers.

Ces directives font l'objet d'un consentement spécifique de la personne concernée et ne peuvent résulter de la seule approbation par celle-ci de conditions générales d'utilisation. Toute clause contractuelle de conditions générales d'utilisation relatives à un traitement portant sur des données à caractère personnel limitant les prérogatives reconnues à la personne en vertu du présent article est réputée non écrite.

Lorsque ces directives prévoient la communication de données qui comportent également des données à caractère personnel relatives à des tiers, cette communication s'effectue dans le respect des dispositions du présent livre.

Le responsable de traitement accuse réception des directives qui lui sont transmises par tout moyen. La personne concernée peut modifier ou révoquer ses directives à tout moment.

Les directives peuvent désigner une personne chargée de leur exécution. Celle-ci a alors qualité, lorsque la personne concernée est décédée, pour prendre connaissance des directives et demander leur mise en œuvre aux responsables de traitement concernés. À défaut de désignation et, sauf directive contraire, ses ayants droit ont qualité pour prendre connaissance des directives au décès de la personne concernée et demander leur mise en œuvre aux responsables de traitement concernés.

Article 53 Gestion des données à caractère personnel en l'absence de directives de la personne concernée

En l'absence de directives ou de mention contraire dans ces directives, les ayants droit de la personne concernée peuvent exercer, après son décès, les droits qui sont conférés à celle-ci par les dispositions du présent chapitre dans la mesure nécessaire :

1) à l'organisation et au règlement de la succession de la personne concernée ; à ce titre, les ayants droit peuvent accéder aux traitements de données à caractère personnel qui la concernent afin d'identifier et d'obtenir communication des informations utiles à la liquidation et au partage de la succession ; ils peuvent aussi recevoir communication des biens numériques ou des données s'apparentant à des souvenirs de famille, transmissibles aux ayants droit ;

2) à la prise en compte, par les responsables de traitement, du décès de la personne concernée ; à ce titre, les ayants droit peuvent faire procéder à la clôture des comptes utilisateurs de la personne concernée, s'opposer à la poursuite des traitements de données à caractère personnel la concernant ou faire procéder à leur mise à jour pour prendre en considération son décès.

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

Les désaccords entre ayants droit sur l'exercice des droits prévus au présent article sont réglés conformément à la loi.

Titre 3 Conditions de réalisation de traitements de données à caractère personnel

Chapitre premier : Principes directeurs, conditions de licéité des traitements de données à caractère personnel

Article 54 Principes relatifs au traitement de données à caractère personnel

Un traitement de données à caractère personnel ne peut valablement être mis en œuvre que si les données à caractère personnel traitées satisfont aux conditions suivantes :

1) elles sont traitées de manière licite, loyale, transparente et non frauduleuse au regard de la personne concernée ;

2) elles sont collectées pour des finalités déterminées, explicites et légitimes, et ne sont pas traitées ultérieurement d'une manière incompatible avec ces finalités ; le traitement ultérieur à des fins de recherche scientifique ou historique ou à des fins statistiques est considéré comme compatible avec les finalités initiales de la collecte s'il est réalisé dans le respect des principes et des procédures prévus au Chapitre 2 et 3 du Titre 3 du présent livreet au Chapitre premier du Titre 2 du présent livreet si ce traitement ultérieur n'est pas utilisé pour prendre des décisions à l'égard des personnes concernées ;

3) elles sont adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées et de leurs traitements ultérieurs ;

4) elles sont exactes, complètes et, si nécessaire, tenues à jour, et toutes les mesures raisonnables sont prises pour que les données à caractère personnel qui sont inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder ;

5) elles sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées ; au-delà de cette période, elles ne peuvent être conservées qu'en vue d'être traitées exclusivement et spécifiquement à des fins de recherche scientifique ou historique ou à des fins statistiques et sous réserve que les mesures techniques et organisationnelles appropriées requises par le présent livre soient mises en œuvre afin de garantir les droits et libertés de la personne concernée ;

6) elles sont traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la destruction, la perte ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées.

Article 55 Conditions de licéité du traitement

Le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie :

1) la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques ;

2) le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ;

3) le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable de traitement ou le destinataire auquel les données sont communiquées est soumis ;

4) le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique ;

5) le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable de traitement ;

6) le traitement est nécessaire afin de répondre aux intérêts légitimes poursuivis par le responsable de traitement ou par le destinataire, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant.

La condition mentionnée au 6) n'est pas susceptible de légitimer les traitements effectués par les autorités publiques dans l'exécution de leurs missions.

Article 56 Conditions de licéité du traitement ultérieur

Lorsque le traitement à une fin autre que celle pour laquelle les données ont été collectées n'est pas fondé sur le consentement de la personne concernée ou sur une obligation légale, le responsable de traitement demande le consentement formel de la personne concernée et, afin de déterminer si le traitement à une autre fin est compatible avec la finalité pour laquelle les données à caractère personnel ont été initialement collectées, tient compte, entre autres :

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

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

3) de la nature des données à caractère personnel, en particulier si le traitement porte sur des catégories particulières de données à caractère personnel visées à l'Article 62 ou si des données à caractère personnel relatives à des condamnations pénales et à des infractions sont traitées conformément à l'Article 63 ;

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

5) de l'existence de garanties appropriées, qui peuvent comprendre le chiffrement ou la pseudonymisation.

Article 57 Caractéristiques du consentement

Le consentement de la personne concernée, afin de valablement légitimer un traitement de données à caractère personnel, doit résulter d'une manifestation de volonté expresse, non équivoque, libre, spécifique et informée par laquelle la personne concernée ou son représentant légal, judiciaire ou conventionnel, accepte que les données à caractère personnel la concernant fassent l'objet d'un traitement manuel ou électronique.

Article 58 Conditions applicables au consentement

Dans les cas où le traitement repose sur le consentement, le responsable de traitement doit être en mesure de démontrer que la personne concernée a donné son consentement au traitement de données à caractère personnel la concernant.

Si le consentement de la personne concernée est donné dans le cadre d'une déclaration écrite qui concerne également d'autres questions, la demande de consentement est présentée sous une forme qui la distingue clairement de ces autres questions, sous une forme compréhensible et aisément accessible, et formulée en des termes clairs et simples. Aucune partie de cette déclaration qui constitue une violation du présent livre n'est susceptible d'avoir un effet contraignant pour la personne concernée.

La personne concernée a le droit de retirer son consentement à tout moment. Le retrait du consentement ne compromet pas la licéité du traitement fondé sur le consentement effectué avant ce retrait mais le responsable doit cesser sans délai tout traitement fondé sur le consentement qui a été retiré. La personne concernée en est informée avant de donner son consentement. Le responsable de traitement est tenu de veiller à ce qu'il soit aussi simple de retirer que de donner son consentement.

Au moment de déterminer si le consentement est donné librement, il y a lieu de tenir le plus grand compte de la question de savoir, entre autres, si l'exécution d'un contrat, y

compris la fourniture d'un service, est subordonnée au consentement à un traitement de données à caractère personnel qui n'est pas nécessaire à l'exécution dudit contrat.

Article 59 Conditions applicables au consentement des mineurs

Le traitement de données à caractère personnel relatives à un mineur en lien avec l'offre de services de la société de l'information ne peut être valablement fondé sur le consentement de la personne concernée tel que prévu au 1) de l'Article 55 que si le mineur ayant consenti au traitement est âgé d'au moins 16 ans, ou si, et dans la mesure où, le consentement est donné ou autorisé par la personne exerçant l'autoritéparentale à l'égard du mineur.

Le cas échéant, le responsable de traitement s'efforce de vérifier que le consentement est donné ou autorisé par la personne exerçant la responsabilité parentale à l'égard du mineur compte tenu des moyens technologiques disponibles.

L'application de cet article au traitement de données à caractère personnel concerné est sans préjudice des règles applicables à la validité, à la formation et aux effets d'un contrat à l'égard d'un mineur.

Article 60 Transparence

Le traitement de données à caractère personnel donne lieu par le responsable de traitement à une information obligatoire des personnes concernées par les traitements qu'il met en œuvre, conformément au Titre 2 du présent livre.

Article 61 Confidentialité et sécurité

Les données à caractère personnel sont traitées de manière confidentielle et protégées conformément aux Article 11,Article 12et Article 13 notamment lorsque le traitement implique la transmission de données dans un réseau.

Article 62 Limites au traitement de données sensibles

Le traitement de données à caractère personnel révélant, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques ou philosophiques, les opinions religieuses ou les croyances ou l'appartenance syndicale d'une personne physique, ainsi que le traitement de données génétiques, de données biométriques aux fins d'identifier une personne physique de manière unique ou de données qui sont relatives à la santé ou à la vie d'une personne physique sont interdits.

L'interdiction prévue au premier alinéa ne s'applique pas dans les cas suivants :

1) la personne concernée a donné son consentement exprès et explicite au traitement pour une ou plusieurs finalités spécifiques, sauf dans le cas où la loi

prévoit que l'interdiction visée au premier alinéa ne peut être levée par le consentement de la personne concernée ;

2) le traitement porte sur des données à caractère personnel manifestement rendues publiques par la personne concernée ;

3) le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique, dans le cas où la personne concernée est dans l'incapacité physique ou juridique de donner son consentement ;

4) le traitement est nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique tels que la protection contre les menaces transfrontalières graves pesant sur la santé, ou aux fins de garantir des normes élevées de qualité et de sécurité des soins de santé et des médicaments ou de dispositifs médicaux sur la base du droit en vigueur dès lors que celui-ci prévoit des mesures appropriées et spécifiques pour la sauvegarde des droits et libertés de la personne concernée, notamment le secret professionnel ;

5) le traitement est nécessaire aux fins de la médecine préventive ou de la médecine du travail, de l'appréciation de la capacité de travail du travailleur, de diagnostics médicaux, de la prise en charge sanitaire ou sociale et de l'administration de soins ou de traitements soit à la personne concernée soit à un parent, ou de la gestion de services de santé et dès lors que le traitement est mis en œuvre par un professionnel de santé soumis au secret professionnel en vertu de la loi ou de règles déontologiques contraignantes et opposables ou sous sa responsabilité ou par une autre personne à laquelle s'impose en raison de ses fonctions une obligation légale ou déontologique contraignante et opposable de secret professionnel ;

6) le traitement est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice ou lorsqu'une juridiction agit dans le cadre de ses fonctions juridictionnelles ;

7) le traitement est mis en œuvre par une association ou tout autre organisme à but non lucratif dont l'objet est de défendre et de promouvoir les libertés et droits fondamentaux dans le cadre de ses activités légitimes correspondant à son objet et avec les garanties appropriées conformément au présent livre, mais à condition que les données à caractère personnel ne soient pas communiquées à des tiers sans le consentement exprès des personnes concernées ;

8) le traitement est nécessaire aux fins de l'exécution des obligations et de l'exercice des droits du responsable de traitement ou de la personne concernée en matière de droit du travail, de sécurité sociale et de protection sociale, dans la mesure où ce traitement est autorisé par la loi ou par une convention collective qui prévoit

des garanties appropriées pour les droits fondamentaux et les intérêts de la personne concernée ;

9) le traitement est mis en œuvre par une association ou tout autre organisme à but non lucratif et à caractère religieux, philosophique, politique ou syndical dans le cadre de ses activités légitimes correspondant à son objet et avec les garanties appropriées conformément au présent livre, mais à condition que :

   a) le traitement ne concerne que les membres ou anciens membres de cette association ou de cet organisme et, le cas échéant, les personnes qui entretiennent avec celui-ci des contacts réguliers dans le cadre de ses activités ; et que

   b) les données à caractère personnel ne soient pas communiquées à des tiers sans le consentement exprès des personnes concernées ;

10) le traitement est nécessaire à des fins de recherche scientifique ou historique ou à des fins statistiques.

L'interdiction prévue au premier alinéa ne s'applique pas non plus aux traitements de données à caractère personnel, automatisés ou non, justifiés par l'intérêt public et autorisés dans les conditions prévues à l'Article 69 et à ceux autorisés par décret dans les conditions prévues à l'Article 71 .

Si les données à caractère personnel visées au premier alinéa sont amenées à faire l'objet à bref délai d'un procédé d'anonymisation préalablement reconnu conforme aux dispositions du présent livre par la Commission, celle-ci peut autoriser, compte tenu de leur finalité, certaines catégories de traitements selon les modalités prévues à l'Article 69. Les dispositions de la Section 1 : Traitements de données à caractère personnel réalisés aux fins de recherche, d'étude ou d'évaluation dans le domaine de la santé et du Chapitre 3 : Formalités particulières et droits spécifiques pour le traitement de certaines catégories de donnéesdu Titre 3 du présent livre ne sont alors pas applicables.

Article 63 Limites au traitement des données relatives aux infractions

Le traitement de données à caractère personnel relatives aux infractions, condamnations pénales et mesures de sûreté ne peut être effectué que par :

1) les juridictions, les autorités publiques et les personnes morales gérant un service public, agissant dans le cadre de leurs attributions légales, notamment leurs missions de police judiciaire ou administrative ; ou

2) les auxiliaires de justice, pour les stricts besoins de l'exercice des missions qui leur sont confiées par la loi, y compris par des avocats ou autres conseils juridiques, pour autant que la défense de leurs clients l'exige.

Article 64 Modalités de collecte particulières

Les données de santé à caractère personnel d'une personne physique sont collectées auprès de la personne concernée. Elles ne peuvent être collectées auprès d'autres personnes qu'à condition que la collecte soit strictement nécessaire aux fins du traitement et que la personne concernée ne soit pas en mesure de fournir les données elle-même.

Sauf consentement exprès de la personne concernée, les données à caractère personnel recueillies par les prestataires de services 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.

Article 65 Décisions individuelles fondées sur un traitement automatisé de données à caractère personnel

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

Aucune décision produisant des effets juridiques à l'égard d'une personne ou l'affectant de manière significative ne peut être prise sur le seul fondement d'un traitement automatisé de données à caractère personnel, y compris sur le fondement d'un traitement destiné à définir le profil de cette personne ou à évaluer certains aspects de sa personnalité. Cette interdiction ne s'applique pas lorsque la décision :

1) est autorisée par la loi, sous réserve que celle-ci prévoie des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée ; ou

2) est fondée sur le consentement explicite de la personne concernée ou est nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et le responsable de traitement, sous réserve que :

   a) le responsable de traitement ait mis en œuvre les mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée, notamment du droit de la personne concernée d'obtenir une intervention humaine de la part du responsable de traitement, d'exprimer son point de vue et de contester la décision ; et que

   b) les règles définissant le traitement ainsi que les principales caractéristiques de sa mise en œuvre aient été communiquées, à l'exception des secrets protégés par la loi, par le responsable de traitement à la personne concernée si elle en a fait la demande.

Les décisions prévues par le deuxième alinéa ne peuvent être fondées sur les catégories particulières de données à caractère personnel visées à l'Article 62 sauf lorsque les cas 1) et 8) dudit article s'appliquent et sous réserve que des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée aient été mises en place.

Chapitre 2 : Formalités préalables à la mise en œuvre de traitements de données à caractère personnel

Section 1 : Régimes applicables

Article 66 Déclaration préalable des traitements

Sauf disposition contraire prévue par le présent Chapitre 2 : Formalités préalables à la mise en œuvre de traitements de données à caractère personnel, les traitements automatisés de données à caractère personnel font l'objet d'une déclaration préalable auprès de la Commission.

La déclaration comporte l'engagement que le traitement de données à caractère personnel satisfait aux exigences du présent livre. La Commission délivre un récépissé, le cas échéant par voie électronique. Le demandeur peut mettre en œuvre le traitement dès réception de ce récépissé. La déclaration n'exonère le demandeur d'aucune de ses responsabilités au titre du présent livre.

Article 67 Déclarations simplifiées

Pour les catégories les plus courantes de traitements de données à caractère personnel, dont la mise en œuvre n'est pas susceptible de porter atteinte à la vie privée ou aux libertés et droits fondamentaux des personnes physiques, la Commission peut établir des normes destinées à simplifier l'obligation de déclaration préalable. La Commission peut soumettre ces normes à consultation publique préalablement à leur établissement. Les normes sont publiées par la Commission.

Ces normes précisent, pour les traitements de données à caractère personnel pouvant faire l'objet d'une déclaration simplifiée :

1) les finalités des traitements autorisées ;

2) les données à caractère personnel ou catégories de données à caractère personnel pouvant être traitées ;

3) la ou les catégories de personnes pouvant être concernées ;

4) les destinataires ou catégories de destinataires auxquels les données à caractère personnel peuvent être communiquées ;

5) la durée autorisée de conservation des données à caractère personnel.

Les traitements de données à caractère personnel qui correspondent à l'une de ces normes font l'objet d'une déclaration simplifiée de conformité transmise à la Commission.

Article 68 Exemption de l'obligation de déclaration

Les traitements de données à caractère personnel pour lesquels le responsable de traitement a désigné un délégué à la protection des données à caractère personnel, conformément au Chapitre 2 : Délégué à la protection des données à caractère personneldu Titre 4du présent livre,sont dispensés de déclaration préalable, sauf lorsqu'un transfert de données à caractère personnel à destination d'un pays tiers, d'une société étrangère ou d'une organisation internationale est envisagé. En cas de non-respect des dispositions du présent livre, le responsable de traitement est tenu de procéder à la déclaration des traitements de données à caractère personnel qu'il effectue et peut y être enjoint par la Commission.

La Commission peut décider, parmi les catégories de traitements pour lesquelles elle a établi une norme destinée à simplifier l'obligation de déclaration préalable conformément à l'Article 67 , d'en dispenser certaines de déclaration, compte tenu de leurs finalités, de leurs destinataires ou catégories de destinataires, des données à caractère personnel traitées, de la durée de conservation de celles-ci et des catégories de personnes concernées.

Article 69 Traitements soumis à autorisation préalable

Les traitements de données à caractère personnel suivants sont soumis à autorisation préalable de la Commission, sauf s'ils relèvent des Article 70,Article 71 et Article 72 :

1) les traitements, automatisés ou non, effectués à des fins de recherche scientifique ou historique ou à des fins statistiques mentionnés au 10) de l'Article 62 ;

2) les traitements, automatisés ou non, pour lesquels les données à caractère personnel sont amenées à faire l'objet à bref délai d'un procédé d'anonymisation conformément au dernier alinéa de l'Article 62 ;

3) les traitements, automatisés ou non, justifiés par l'intérêt public conformément à l'avant-dernier alinéa de l'Article 62 ;

4) les traitements automatisés portant sur des données génétiques, à l'exception des traitements 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 ;

5) 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 des auxiliaires de justice pour les besoins de leurs missions de défense des personnes concernées ;

6) 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 établissant cette exclusion ;

7) les traitements automatisés ayant pour objet :

   a) l'interconnexion de fichiers relevant d'une ou de plusieurs personnes morales gérant un service public et dont les finalités correspondent à des intérêts publics différents ; ou

   b) l'interconnexion de fichiers relevant d'autres personnes et dont les finalités principales sont différentes ;

8) les traitements portant sur des données à caractère personnel parmi lesquelles figure le numéro national d'identification de personnes physiques inscrit au registre national des personnes physiques conformément à la loi n° 39/AN/19/8ème L du 21 janvier 2019 portant identification des personnes physiques en République de Djibouti, création du numéro national d'identification et établissement d'un registre national, et ceux qui requièrent une consultation de ce registre sans inclure le numéro national d'identification de personnes physiques ;

9) les traitements automatisés de données à caractère personnel comportant des appréciations sur les difficultés sociales des personnes ;

10) les traitements automatisés comportant des données biométriques nécessaires au contrôle de l'identité des personnes.

Article 70 Traitements mis en œuvre par voie réglementaire

Les traitements de données à caractère personnel mis en œuvre pour le compte de l'État, d'une personne morale de droit public ou d'une personne morale de droit privé gérant un service public sont mis en œuvre dans les conditions fixées par les Article 71 et Article 72selon que ces traitements entrent dans les catégories de traitements mentionnées dans chacun de ces articles.

En cas de conflit d'application entre ces articles pour déterminer l'acte réglementaire approprié pour autoriser un traitement, il est systématiquement recouru à l'acte réglementaire de valeur normative supérieure.

Article 71 Traitements mis en œuvre par voie réglementaire simple

Les traitements de données à caractère personnel suivants mis en œuvre pour le compte de l'État sont autorisés par voie réglementaire:

1) les traitements qui intéressent la sûreté de l'État, la défense ou la sécurité publique, dans ce cas sur proposition du ministre chargé de l'intérieur ; ou

2) les traitements 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.

Par exception à ce qui précède, lorsque ces traitements portent sur des catégories de données à caractère personnel mentionnées à l'Article 62 , ils sont autorisés par décret pris après avis motivé de la Commission.

L'avis de la Commission est publié avec l'arrêté ou le décret autorisant le traitement.

Certains des traitements visés au présent article peuvent être dispensés de la publication de l'acte réglementaire qui les autorise par décret pris en Conseil des ministres. Pour ces traitements, seul le sens de l'avis émis par la Commission est publié avec le décret autorisant la dispense de publication de l'acte réglementaire.

Article 72 Traitements mis en œuvre par voie réglementaire renforcée

Les traitements de données à caractère personnel suivants mis en œuvre pour le compte de l'État sont autorisés par décret après avis motivé de la Commission :

1) les traitements d'une personne morale de droit public ou d'une personne morale de droit privé gérant un service public qui portent sur des données à caractère personnel parmi lesquelles figure le numéro national d'identification de personnes physiques inscrit au registre national des personnes physiques conformément à la loi n° 39/AN/19/8ème L du 21 janvier 2019 portant identification des personnes physiques en République de Djibouti, création du numéro national d'identification et établissement d'un registre national ;

2) les traitements qui portent sur des données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes.

Par exception à ce qui précède, les traitements de données à caractère personnel suivants sont autorisés par arrêté ou, en cas de traitement mis en œuvre 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 direction, dans chaque cas, après avis motivé de la Commission :

1) les traitements mis en œuvre par l'État ou par une personne morale de droit public ou une personne morale de droit privé gérant un service public qui requièrent une consultation du registre national des personnes physiques sans inclure le numéro national d'identification inscrit à ce registre ;

2) les traitements mentionnés au premier alinéa qui :

   a) ne comportent aucune des données sensibles mentionnées à l'Article 62 ou relatives aux infractions mentionnées à l'Article 63 ; et

   b) ne donnent pas lieu à une interconnexion entre des traitements ou fichiers correspondant à des intérêts publics différents ; et

   c) sont mis en œuvre par une personne morale de droit public ou une personne morale de droit privé gérant un service public 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 ;

3) les traitements relatifs au recensement de la population ;

4) les traitements mis en œuvre par l'État ou par une personne morale de droit public ou une personne morale de droit privé gérant un service public aux fins de mettre à la disposition des administrés un ou plusieurs téléservices de l'administration électronique conformément au Titre 1 du Livre Septième , si ces traitements portent sur des données à caractère personnel parmi lesquelles figurent le numéro national d'identification de personne physiques ou tout autre identifiant des personnes physiques.

L'avis de la Commission est publié avec l'arrêté ou le décret autorisant le traitement.

Article 73 Dispense de formalités préalables

Les traitements de données à caractère personnel suivants ne sont soumis à aucune des formalités préalables prévues au présent Chapitre 2 : Formalités préalables à la mise en œuvre de traitements de données à caractère personnel:

1) 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 ;

2) les traitements mis en œuvre par une association ou tout organisme à but non lucratif et à caractère religieux, philosophique, politique ou syndical, dès lors que ces données correspondent à l'objet de cette association ou de cet organisme,

qu'elles ne concernent que leurs membres et qu'elles ne sont pas communiquées à des tiers ; et

3) les traitements dont la finalité se limite à assurer la conservation à long terme de documents d'archives publiques.

Le responsable d'un traitement de données à caractère personnel 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 mentionnées aux 3) à 8) l'Article 126.

Section 2 : Modalités d'application

Article 74 Contenu des déclarations et des dossiers de demande

Les déclarations, déclarations simplifiées demandes d'autorisation et demandes d'avis adressées à la Commission en application des dispositions de la Section 1 comportent les informations précisées par voie réglementaire.

Les demandes d'avis portant sur les traitements intéressant la sûreté de l'État, la défense ou la sécurité publique peuvent ne pas comporter tous les éléments d'information énumérés ci-dessus. Un décret pris en Conseil des ministres, pris après avis de la Commission, fixe la liste de ces traitements et des informations que les demandes d'avis portant sur ces traitements doivent comporter au minimum.

Article 75 Modalités de saisine et de transmission des dossiers à la Commission

Les déclarations et les déclarations simplifiées et les demandes d'autorisation peuvent être adressées à la Commission par voie électronique.

Article 76 Délais d'instruction

Lorsque la déclaration comporte l'engagement prévu au deuxième alinéa de l'Article 66 et satisfait aux prescriptions de l'Article 74 ou lorsque le traitement déclaré répond aux normes établies par la Commission en vertu de l'Article 67 , la Commission délivre sans délai le récépissé prévu par l'Article 66 .

Dans les autres cas, la Commission se prononce dans les délais fixés par décret pris en Conseil des ministres.

Article 77 Déclarations et autorisations uniques

Les traitements de données à caractère personnel visés à l'Article 66 relevant d'un même organisme 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 74 ne sont fournies pour chacun des traitements que dans la mesure où elles lui sont propres.

La Commission peut autoriser les responsables de certaines catégories de traitements visées à l'Article 67 à procéder à une déclaration simplifiée unique conformément au premier alinéa du présent article et au vu des conditions établies au dernier alinéa de l'Article 68 .

Les traitements de données à caractère personnel visés à l'Article 69 qui répondent à une même finalité, portent sur des catégories de données identiques et ont les mêmes destinataires ou catégories de destinataires peuvent être autorisés par une décision unique de la Commission. Dans ce cas, le responsable de chaque traitement adresse à la Commission un engagement de conformité de celui-ci à la description figurant dans l'autorisation.

Les traitements de données à caractère personnel visés aux Article 70, Article 71 et Article 72 qui répondent à une même finalité, portent sur des catégories de 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 la Commission un engagement de conformité de celui-ci à la description figurant dans l'acte réglementaire.

Article 78 Modification des informations relatives à un traitement déclaré ou autorisé

Le responsable d'un traitement déjà déclaré ou autorisé informe dans un délai de dix (10) jours la Commission de tout changement affectant les informations mentionnées à l'Article 74 ainsi que, le cas échéant, de la suppression du traitement.

Article 79 Contenu des actes d'autorisation

Les actes autorisant la création d'un traitement en application des Article 69, Article 70, Article 71 et Article 72 indiquent :

1) la dénomination et la finalité du traitement ;

2) le service auprès duquel peuvent être exercés les droits de la personne concernée conformément au Chapitre 2 du Titre 2 du présent livre et ses coordonnées ;

3) les catégories de données à caractère personnel enregistrées ;

4) les destinataires ou catégories de destinataires habilités à recevoir communication de ces données ;

5) le cas échéant, les dérogations au droit à l'information prévues à l'Article 88 qui s'appliquent.

Chapitre 3 : Formalités particulières et droits spécifiques pour le traitement de certaines catégories de données

Section 1 : Traitements de données à caractère personnel réalisés aux fins de recherche, d'étude ou d'évaluation dans le domaine de la santé

Article 80 Application des dispositions du présent livre aux traitements aux fins de recherche dans le domaine de la santé ou de suivi

Les traitements automatisés de données à caractère personnel ayant pour finalité la recherche ou les études dans le domaine de la santé ainsi que l'évaluation ou l'analyse des pratiques ou des activités de soin ou de prévention sont soumis aux dispositions du présent livre, à l'exception des dispositions du Chapitre 2 du Titre 3 et des dispositions des Sections 1 et 3 du Chapitre 2 du Titre 2 du présent livre auxquelles la présente section déroge s'agissant de ces traitements.

La présente section n'est pas applicable aux traitements de données à caractère personnel suivants, qui restent régis par les autres dispositions du présent livre qui s'y appliquent le cas échéant :

1) les traitements ayant pour finalité le suivi thérapeutique ou médical individuel des patients ;

2) les traitements permettant d'effectuer des études à partir des données recueillies dans le cadre de traitements mentionnés au 1) lorsque ces études sont réalisées par les personnels assurant le suivi et destinées à leur usage exclusif ;

3) les traitements effectués à des fins de remboursement ou de contrôle par les organismes chargés de la gestion d'un régime de base d'assurance maladie obligatoire ainsi que la prise en charge des prestations par les organismes d'assurance maladie complémentaire ;

4) les traitements effectués au sein des établissements de santé par les médecins responsables de l'information dans le respect du secret médical et des droits des patients en vue d'améliorer la connaissance et l'évaluation de l'activité et des coûts et de favoriser l'optimisation de l'offre de soins ;

5) les traitements effectués par les agences de santé et par l'État ou toute personne publique désignée par lui ayant pour finalité d'élaborer le projet national de santé et de déterminer les ressources des établissements de santé, l'évaluation de la qualité des soins, la veille et la vigilance sanitaire ainsi que le contrôle de l'activité de soin et de la facturation des établissements de santé ;

6) les traitements ayant pour finalité de répondre à une alerte sanitaire et d'en gérer les suites effectués par les organismes ou les services chargés d'une mission de service public figurant sur une liste fixée par arrêtés des Ministres en charge de la

santé et de la sécurité sociale pris après avis de la Commission dans les conditions prévues au Chapitre 2 du Titre 3 du présent livre.

Article 81 Vérifications opérées par la Commission et autorisation des traitements

Les traitements de données à caractère personnel mentionnés au premier alinéa de l'Article 80 ne peuvent être mis en œuvre qu'en considération de la finalité d'intérêt public la recherche, l'étude ou l'évaluation ou le suivi poursuit et sont soumis à autorisation préalable de la Commission dans le respect des principes définis par le présent livre et compte tenu de cet intérêt public. La garantie de normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux constitue une finalité d'intérêt public.

La Commission vérifie les garanties présentées par le demandeur pour l'application des dispositions du présent livre et en particulier de la présente section et la conformité de sa demande à ses missions ou à son objet social. Si le demandeur n'apporte pas d'éléments suffisants pour attester la nécessité de disposer de certaines informations parmi l'ensemble des données à caractère personnel dont le traitement est envisagé, la Commission peut interdire la communication de ces informations par l'organisme qui les détient et n'autoriser le traitement que pour ces données réduites.

La Commission statue sur la durée de conservation des données nécessaires au traitement et apprécie les dispositions prises pour assurer leur sécurité conformément aux dispositions du présent livre et la garantie des secrets protégés par la loi.

La Commission se prononce dans les conditions prévues à l'Article 76 .

Article 82 Avis préalable d'un comité consultatif

La Commission prend sa décision après avis d'un comité consultatif. Ce comité est composé de personnes choisies en raison de leur compétence dans une pluralité de disciplines, notamment en matière de recherche dans le domaine de la santé, d'épidémiologie, de génétique et de biostatistique. Le comité peut comprendre plusieurs Sections compétentes en fonction de la nature ou de la finalité des traitements. La composition du comité et ses règles de fonctionnement sont définies par décret pris en conseil des ministres, après avis de la Commission. Ce décret fixe les règles relatives aux conflits d'intérêt auxquelles sont soumis les membres du comité.

Le comité consultatif émet un avis sur la méthodologie retenue pour la recherche, l'étude ou l'évaluation, sur le caractère d'intérêt public que représente la recherche, l'étude ou l'évaluation justifiant la demande de traitement, sur la nécessité du recours à des données à caractère personnel, sur la pertinence de celles-ci par rapport à la finalité du traitement, et, s'il y a lieu, sur la qualité scientifique du projet. Le cas échéant, le

comité recommande aux demandeurs des modifications de leur projet afin de le mettre en conformité avec les obligations prévues par le présent livre.

Le comité rend son avis dans un délai d'un mois à compter de sa saisine. À défaut d'avis dans ce délai, l'avis est réputé favorable. En cas d'urgence, ce délai peut être ramené à quinze (15) jours.

Les dossiers de demandes d'autorisation sont transmis à la Commission qui en transmet immédiatement une copie au comité consultatif pour avis. Le délai imparti au comité pour rendre son avis court à compter de la réception du dossier par celui-ci.

Article 83 Méthodologies de référence

Pour les catégories les plus usuelles de traitements automatisés de données de santé à caractère personnel à des fins de recherche, d'étude ou d'évaluation ou de suivi dans le domaine de la santé, la Commission peut homologuer et publier des méthodologies de référence destinées à simplifier la procédure d'examen.

Ces méthodologies sont établies en concertation avec le comité consultatif et des organismes publics et privés représentatifs des acteurs concernés.

Lorsque le traitement est conforme à une méthodologie de référence, il peut être mis en œuvre sans autorisation, à la condition que le responsable de traitement adresse préalablement à la Commission une déclaration attestant de cette conformité dans les conditions prévues à l'Article 75 .

Article 84 Exemption d'autorisation des jeux de données agrégées et échantillons

Des jeux de données agrégées ou des échantillons, issus des traitements des données de santé à caractère personnel effectués pour des finalités et dans des conditions reconnues conformes au présent livre par la Commission, peuvent faire l'objet d'une mise à disposition, dans des conditions préalablement homologuées par la Commission, sans que l'autorisation prévue à l'Article 81 ne soit requise.

Article 85 Autorisations uniques

Les traitements de données à caractère personnel visés à l'Article 81 qui répondent à une même finalité, portent sur des catégories de données identiques et ont les mêmes destinataires ou catégories de destinataires peuvent être autorisés par une décision unique de la Commission délivrée à un même demandeur.

Article 86 Conditions de transmission pour traitement des données détenues par les professionnels de santé

Nonobstant les règles relatives au secret professionnel, les professionnels de santé peuvent transmettre les données à caractère personnel qu'ils détiennent dans le cadre d'un traitement autorisé en application de l'Article 81.

Lorsque ces données permettent l'identification des personnes, leur transmission doit être effectuée dans des conditions de nature à garantir leur confidentialité. La Commission adopte des recommandations ou des référentiels sur les procédés techniques à mettre en œuvre.

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

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

Les personnes appelées à mettre en œuvre le traitement de données ainsi que celles qui ont accès aux données sur lesquelles il porte sont astreintes au secret professionnel dans les conditions prévues par la loi.

Article 87 Droit d'information spécifique

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

1) de la nature des données transmises ;

2) la ou les finalités déterminées poursuivies par le traitement auquel les données à caractère personnel sont destinées ;

3) les destinataires des données à caractère personnel auxquels celles-ci sont communiquées ;

4) des droits d'accès, de rectification et d'effacement dont elles jouissent en qualité de personne concernée institués aux Sections 2, 4 et 5 du Chapitre 2 du Titre 2 du présent livre;

5) de leur droit d'opposition institué aux deuxième et troisième alinéas de l'Article 89 ou, dans le cas prévu au premier alinéa de cet article, de l'obligation de recueillir leur consentement.

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

Article 88 Limites au droit d'information

Lorsque les données à caractère personnel ont été initialement recueillies pour une autre finalité que la recherche, l'étude ou l'évaluation ou le suivi, il peut être dérogé à l'obligation d'information établie par l'Article 87 :

1) pour les traitements nécessaires à la conservation de ces données à des fins historiques, statistiques ou scientifiques, dans les conditions prévues par la loi ;

2) lorsque l'information individuelle se heurte à la difficulté de retrouver les personnes concernées.

Les demandes de dérogation à l'obligation d'informer les personnes concernées de l'utilisation de données les concernant à des fins de recherche, d'étude ou d'évaluation sont justifiées dans le dossier de demande d'autorisation transmis à la Commission qui statue sur ce point.

Lorsque les recherches, les études, les évaluations ou les suivis recourent à des données de santé à caractère personnel non directement identifiantes recueillies à titre obligatoire et destinées aux services, aux établissements de l'État, des collectivités territoriales ou aux organismes de sécurité sociale, l'information des personnes concernées quant à la réutilisation possible de ces données, à des fins de recherche, d'étude, d'évaluation ou de suivi et aux modalités d'exercice de leurs droits est assurée selon des modalités définies par décret en Conseil des ministres après avis de la Commission. Ces modalités peuvent inclure :

1) une information sur le site Internet des établissements de santé, des établissements médico-sociaux, des organismes de sécurité sociale, d'assurance maladie obligatoire ou d'assurance maladie complémentaire ;

2) d'affiches dans les locaux ouverts au public ;

3) de documents remis aux personnes concernées.

Article 89 Consentement et droit d'opposition spécifique

Dans le cas où la recherche nécessite le recueil de prélèvements biologiques identifiants ou l'examen de caractéristiques génétiques, le consentement éclairé et exprès des personnes concernées doit être obtenu sous forme écrite préalablement à la mise en œuvre du traitement.

Toute personne a le droit de s'opposer à ce que des données à caractère personnel la concernant fassent l'objet de la levée du secret professionnel rendue nécessaire par un traitement visé à l'Article 86. Cette opposition s'effectue par tout moyen après soit du responsable de traitement, soit de l'établissement ou du professionnel de santé détenteur de ces données.

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

Article 90 Autres destinataires des informations et exerçants les droits de la personne concernée

S'agissant des mineurs et des personnes faisant l'objet d'une mesure de tutelle, les informations prévues à l'Article 87 sont communiquées respectivement aux titulaires de l'exercice de l'autorité parentale et au représentant légal, et les droits prévus à l'Article 89 sont exercés par ces derniers.

Par dérogation, pour les traitements de données à caractère personnel effectués dans le cadre d'études ou d'évaluations dans le domaine de la santé ayant une finalité d'intérêt public et incluant des personnes mineures, l'information préalable prévue à l'Article 87 peut être effectuée auprès d'un seul des titulaires de l'exercice de l'autorité parentale, s'il est impossible d'informer l'autre titulaire ou s'il ne peut être consulté dans des délais compatibles avec les exigences méthodologiques propres à la réalisation de l'étude ou de l'évaluation au regard de ses finalités. Le présent alinéa ne fait pas obstacle à l'exercice ultérieur, par chaque titulaire de l'exercice de l'autorité parentale, des droits d'accès, de rectification et d'opposition.

Article 91 Affichage des informations dans les lieux de santé

Une information relative aux dispositions de la présente section doit être assurée dans tout établissement ou centre de santé où s'exercent des activités de prévention, de diagnostic et de soins donnant lieu à la transmission de données à caractère personnel en vue d'un traitement visé à l'Article 80.

Article 92 Retrait automatique de l'autorisation en cas de violation

La mise en œuvre d'un traitement de données à caractère personnel en violation des conditions prévues par la présente section entraîne le retrait temporaire ou définitif par la Commission de l'autorisation délivrée en application de l'Article 81 .

Il en est de même en cas de refus de se soumettre aux vérifications effectuées sur le traitement par la Commission conformément au présent livre.

Article 93 Régime spécifique d'autorisation des transferts vers des pays tiers

La transmission vers un pays tiers de données à caractère personnel non codées faisant l'objet d'un traitement à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé est spécifiquement autorisée dans les conditions prévues aux Article 81 et Article 82 et sous réserve du respect des dispositions de la Section 2 du Chapitre 4 du Titre 3.

Section 2 : Traitement aux fins de journalisme et d'expression littéraire et artistique

Article 94 Application des dispositions de la loi aux traitements réalisés aux fins de journalisme et d'expression littéraire et artistique

À titre dérogatoire, le 5) de l'Article 54 , les Article 62,Article 63 etArticle 66 les 1), 2), 3) et 5) de l'Article 80, les Sections 1, 2 et 4 du Chapitre 2 du Titre 2, et la Section 2 du Chapitre 4 du Titre 3 du présent livre ne s'appliquent pas, lorsqu'une telle dérogation est nécessaire pour concilier le droit à la protection des données à caractère personnel et la liberté d'expression et d'information, aux traitements de données à caractère personnel mis en œuvre aux seules fins :

1) d'expression littéraire et artistique ;

2) d'exercice, à Titre professionnel, de l'activité de journaliste, dans le respect des règles déontologiques de cette profession.

Article 95 Tenue d'un registre des traitements aux fins de journalisme par les responsables de traitement

Pour les traitements mentionnés au 2) de l'Article 80 , la dispense de l'obligation de déclaration prévue par l'Article 66 est subordonnée à la désignation par le responsable de traitement d'un délégué à la protection des données appartenant à un organisme de la presse écrite ou audiovisuelle conformément aux dispositions du Chapitre 2 du Titre 4 du présent livre, et à la tenue par celui-ci d'un registre des traitements mis en œuvre par le responsable de traitement.

Les dispositions du Chapitre 2 du Titre 4 du présent livre s'appliquent.

Article 96 Articulation avec les dispositions applicables en matière de presse, d'audiovisuel et en matière pénale

Les dispositions de la présente section ne font pas obstacle à l'application des dispositions légales qui prévoient les conditions d'exercice du droit de réponse et qui préviennent, limitent, réparent et, le cas échéant, répriment les atteintes à la vie privée et à la réputation des personnes.

Chapitre 4 : Interconnexion et transfert de données à caractère personnel

Section 1 : Interconnexion des données à caractère personnel

Article 97 Légitimité de l'interconnexion de fichiers comportant des données à caractère personnel

L'interconnexion de fichiers comportant des données à caractère personnel 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 ou de réduction des droits, libertés et garanties pour les personnes concernées. Elle doit être assortie de mesures de sécurité appropriées et tenir compte du principe de pertinence des données faisant l'objet de l'interconnexion.

Article 98 Autorisation préalable de l'interconnexion de fichiers comportant des données à caractère personnel

L'interconnexion de fichiers comportant des données à caractère personnel relevant d'une ou plusieurs personnes morales gérant un service public et dont les finalités correspondent à des intérêts publics différents et l'interconnexion de fichiers relevant d'autres personnes et dont les finalités principales sont différentes sont soumises à autorisation de la Commission délivrée dans les conditions prévues par le Chapitre 2 du Titre 3 du présent livre.

L'interconnexion de fichiers comportant des données à caractère personnel est inscrite au registre national des traitements de données à caractère personnel dans les conditions prévues par le Chapitre 3 du Titre 4 du présent livre.

Section 2 : Transfert de données à caractère personnel vers un pays tiers ou une organisation internationale

Article 99 Admissibilité des transferts vers un pays tiers ou une organisation internationale présentant un niveau de protection adéquat

Le responsable de traitement ou le sous-traitant le cas échéant ne peut transférer de données à caractère personnel vers un pays tiers ou une organisation internationale en vue d'un traitement après leur transfert que si le pays ou l'organisation en question assure un niveau de protection de la vie privée, des libertés et droits fondamentaux des personnes physiques équivalent et suffisant par rapport à celui mis en place par les dispositions du présent livre à l'égard du traitement dont ces données font l'objet ou peuvent faire l'objet.

Les transferts ultérieurs de données à caractère personnel au départ du pays tiers ou de l'organisation international vers un autre pays tiers ou une autre organisation internationale doivent satisfaire les mêmes exigences.

Article 100 Détermination de l'adéquation du niveau de protection

Le caractère équivalent et suffisant du niveau de protection s'apprécie au regard de toutes les circonstances relatives à un transfert de données ou à une catégorie de transferts de données, notamment des caractéristiques propres du traitement en cause telles que sa finalité et sa durée ainsi que la nature, l'origine et la destination des données traitées. Afin de déterminer ce caractère équivalent et suffisant, il est également tenu compte :

1) de l'état de droit, du respect des libertés et droits fondamentaux, de la législation pertinente, tant générale que sectorielle, notamment dans le domaine de la sécurité publique, de la défense, de la sécurité nationale et du droit pénal ainsi que l'accès des autorités publiques aux données à caractère personnel, de même que de la mise en œuvre de ladite législation, des règles en matière de protection des données à caractère personnel, des règles professionnelles et des mesures de sécurité, y compris des règles relatives au transfert ultérieur de données à caractère personnel vers un autre pays tiers ou à une autre organisation internationale qui sont respectées dans le pays tiers ou par l'organisation internationale en question, de la jurisprudence, ainsi que des droits effectifs et opposables dont bénéficient les personnes concernées et des recours administratifs et judiciaires que peuvent effectivement introduire les personnes concernées dont les données à caractère personnel sont transférées ;

2) de l'existence et du fonctionnement effectif d'une ou de plusieurs autorités de contrôle indépendantes dans le pays tiers, ou auxquelles une organisation internationale est soumise, chargées d'assurer le respect des règles en matière de protection des données à caractère personnel et de les faire appliquer, d'assister et de conseiller les personnes concernées dans l'exercice de leurs droits ; et

3) des engagements internationaux pris par le pays tiers ou l'organisation internationale en question, ou d'autres obligations découlant de conventions ou d'instruments juridiquement contraignants ainsi que de sa participation à des systèmes multilatéraux ou régionaux, en particulier en ce qui concerne la protection des données à caractère personnel.

La Commission apprécie le niveau de protection offert par les pays et les organisations internationales vers lesquels un transfert de données à caractère personnel est envisagé.

Elle publie la liste des pays et organisations internationales qu'elle a reconnues comme assurant un niveau de protection suffisant à l'égard d'un transfert ou d'une catégorie de transferts de données à caractère personnel.

La Commission réévalue son appréciation pour chaque pays et organisation internationale autant que de besoin en fonction des évolutions des conditions s'appliquant au transfert et au traitement des données à caractère personnel et au moins tous les trois (3) ans.

Article 101 Interdiction et cessation des transferts en l'absence d'un niveau de protection adéquat

Si la Commission estime qu'un pays ou une organisation internationale n'assure pas ou n'assure plus un niveau de protection suffisant à l'égard d'un transfert ou d'une catégorie de transferts de données à caractère personnel, la Commission :

1) retire ce pays ou cette organisation de la liste mentionnée à l'Article 100 ;

2) saisie d'une déclaration déposée en application des Article 66 et Article 67 faisant apparaître que des données à caractère personnel seront transférées vers ce pays ou cette organisation internationale, délivre le récépissé avec mention de l'interdiction de procéder au transfert des données ;

3) enjoint à tout responsable de traitement de cesser tout transfert de données à caractère personnel existant vers ce pays ou cette organisation internationale.

Article 102 Autorisation des transferts vers un pays tiers ou une organisation internationale n'assurant pas un niveau de protection adéquat

Le responsable de traitement ou le sous-traitant peut procéder au transfert ou à une catégorie de transferts de données à caractère personnel vers un pays tiers non membre de l'Union Africaine ou une organisation internationale n'assurant pas un niveau de protection adéquat et suffisant dans les cas suivants :

1) la personne concernée a expressément donné son consentement au transfert envisagé ;

2) le transfert est nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable de traitement ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ;

3) le transfert est nécessaire à la conclusion ou à l'exécution d'un contrat conclu ou à conclure dans l'intérêt de la personne concernée entre le responsable de traitement et un tiers ;

4) le transfert est nécessaire ou rendu juridiquement obligatoire pour la sauvegarde de l'intérêt public ;

5) le transfert est nécessaire pour la constatation, l'exercice ou la défense d'un droit en justice ;

6) le transfert est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'autres personnes, lorsque la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement ;

7) le transfert est nécessaire à la consultation, dans des consultations régulières, d'un registre public qui, en vertu de 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, dans la mesure où les conditions légales pour la consultation sont remplies dans le cas particulier.

Hors les cas prévu par le présent article, la Commission peut autoriser un transfert ou un ensemble de transfert de données à caractère personnel vers un pays tiers ou une organisation n'assurant pas un niveau de protection adéquat et suffisant lorsque le responsable de traitement offre des garanties suffisantes au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes concernées ainsi qu'à l'égard de l'exercice par celles-ci des droits dont elles jouissent en cette qualité en vertu du présent livre. Pour les traitements mentionnés à l'Article 71, le transfert peut être autorisé par décret pris en Conseil des ministres dans les conditions prévues par cet article lorsque le traitement présente les mêmes garanties.

Article 103 Contrôle des transferts

Les transferts de données à caractère personnel vers des pays tiers ou une organisation internationale font l'objet d'un contrôle régulier de la Commission au regard de leur finalité.

Titre 4 Contrôle et sanctions

Chapitre premier : La Commission Nationale de Protection des Données à Caractère Personnel

Section 1 : Dispositions générales

Article 104 Création et statut de la Commission

Il est créé une autorité administrative indépendante chargée de veiller à ce que les traitements de données à caractère personnel soient mis en œuvre conformément aux dispositions du présent livre dénommée Commission Nationale de Protection des Données à Caractère Personnel.

Elle informe les personnes concernées et les responsables de traitement de leurs droits et obligations et s'assure que les TIC ne comportent pas de menace au regard des libertés publiques et de la vie privée.

La Commission est une personne morale de droit public indépendante, dotée de la personnalité juridique et jouissant de l'autonomie administrative, financière.

Le siège de la Commission est fixé à Djibouti. Il peut être transféré en cas de besoin en tout autre lieu du territoire national par décret.

Article 105 Missions

La Commission Nationale de Protection des Données à Caractère Personnel garantit la préservation des libertés et droits fondamentaux des personnes physiques et en particulier leur vie privée et assure leur protection dans le cadre des traitements de données à caractère personnel les concernant.

À ce titre, elle exerce les missions qui lui sont conférées par le présent livre et est en particulier chargée, dans les conditions prévues par le présent livre :

1) d'informer les personnes concernées et les responsables de traitements et les sous-traitants de leurs droits et obligations ;

2) de sensibiliser le public aux risques liés au traitement de données à caractère personnel et aux meilleures pratiques en vue de leur protection ;

3) de promouvoir l'utilisation des technologies protectrices de la vie privée, notamment les technologies de chiffrement des données ;

4) de veiller à ce que les traitements de données à caractère personnel soient créés et effectués conformément aux dispositions du présent livre, et de contrôleur leur mise en œuvre ;

5) de recevoir les déclarations préalables, d'octroyer les autorisations et de répondre à toute demande d'avis pour la mise en œuvre de traitement de données à caractère personnel ;

6) d'autoriser, l'interconnexion de fichiers et les transferts de données à caractère personnel vers des pays tiers , des sociétés étrangères et des organisations internationales ;

7) de recevoir les réclamations, pétitions et plaintes relatives à la mise en œuvre des traitements de données à caractère personnel et d'informer leurs auteurs des suites données à celles-ci ;

8) de répondre aux demandes d'avis des autorités publiques et des juridictions ;

9) de conseiller les personnes et organismes qui procèdent à des traitements de données à caractère personnel ou qui souhaitent procéder à des essais ou expériences en la matière ;

10) de procéder, par le biais d'agents assermentés, à des vérifications portant sur tout traitement de données caractère personnel soumis aux dispositions du présent livre et relevant de ses prérogatives ;

11) d'informer, sans délai, le procureur de la République, conformément aux dispositions de l'article 37 du code de procédure pénale, des violations des dispositions du présent livre dont elle a connaissance ;

12) d'établir, de tenir à jour et de mettre à disposition du public pour consultation le registre national des traitements de données à caractère personnel prévu par les Article 125 et Article 126.

La Commission est consultée sur tout projet de texte législatif ou réglementaire en rapport avec la protection des libertés et droits fondamentaux des personnes physiques en lien avec des traitements de données à caractère personnel. Ses avis peuvent être rendus publics.

La Commission peut, de sa propre initiative, faire des propositions susceptibles de simplifier et d'adapter le cadre législatif et règlementaire concernant le traitement des données à caractère personnel et la protection des libertés individuelles, notamment compte tenu de l'évolution des procédés et techniques informatiques.

La Commission met en place des mécanismes de coopération avec les autorités de contrôle des traitements de données à caractère personnel d'autres pays et peut, sur demande du gouvernement, participer à la préparation et à la définition de la position djiboutienne dans les négociations internationales en matière de protection des données à caractère personnel.

La Commission adopte des lignes directrices, recommandations et référentiels destinés à faciliter la mise en œuvre du présent livre par les responsables de traitement et les sous-traitants et l'exercice de leurs droits par les personnes concernées.

Section 2 : Organisation

Article 106 Composition

Les membres de la Commission sont choisis pour leur impartialité, leur probité et leur compétence dans les domaines technique, juridique, judiciaire et informatique ou en lien aux questions touchant aux libertés individuelles.

La Commission est composée de douze (12) membres désignés comme suit :

1) trois (3) personnalités qualifiées désignées par le Président de la République, dont au moins un (1) expert en technologie de l'information et de la communication ;

2) trois (3) députés désigné sur proposition du président de l'Assemblée Nationale ;

3) trois (3) magistrats, dont au moins un ayant siégé en matière administrative, désignés sur proposition du premier président de la Cour Suprême ;

4) une (1) personnalité qualifiée désignée par le Ministre chargé de l'économie numérique ;

5) une (1) personnalité qualifiée désignée sur proposition du président de la Commission Nationale des Droits de l'Homme.

6) Une (1) personnalité qualifiée désignée par l'association des entreprises.

Article 107 Nomination et prérogatives des membres de la Commission

Pour être nommé membre de la Commission, il faut être de nationalité djiboutienne, jouir de ses droits civils et politiques, présenter les qualités exposées à l'Article 106 et ne pas relever des cas d'incompatibilité mentionnés à l'Article 108 .

Les membres de la Commission sont désignés par décret pris en Conseil des ministres. Le président de la Commission est désigné par le Président de la République. La Commission élit parmi ses membres deux vices présidents dont un vice-président délégué.

Le président est chargé de la gestion quotidienne des affaires de la Commission et de l'exécution de ses décisions. La Commission peut charger le président ou l'un de ses vice-présidents d'exercer tout ou partie de ses attributions. Le président peut déléguer tout ou partie de ses attributions aux vice-présidents ou à tout autre agent de la Commission. En cas d'empêchement du président, le vice-président délégué exerce les attributions du président.

L'ordre du jour des séances de la Commission est public.

Article 108 Incompatibilités

La qualité de membre de la Commission est incompatible avec celle de membre du gouvernement et la détention, directe ou indirecte, d'intérêts dans une entreprise du secteur des communications électroniques ou des technologies de l'information et de la communication ou de l'informatique.

À l'exception du président, les membres de la Commission n'exercent pas leurs fonctions à titre exclusif. Toutefois, les membres de la Commission s'abstiennent de tout acte incompatible avec leurs fonctions et, pendant la durée de leur mandat, n'exercent aucune activité professionnelle incompatible, rémunérée ou non.

Le président de la Commission exerce ses fonctions à plein temps. La fonction de président est incompatible avec toute autre activité professionnelle ou tout autre emploi public.

Aucun membre de la Commission ne peut :

1) 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 ;

2) 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 fonction ou détenu un mandat.

Tout membre de la Commission doit informer le président des intérêts directs ou indirects qu'il détient ou vient à détenir, des fonctions qu'il exerce ou vient à exercer et de tout mandat qu'il détient ou vient à détenir au sein d'une personne morale. Ces informations, ainsi que celles concernant le président, sont tenues à la disposition des membres de la Commission.

Le président de la Commission prend les mesures appropriées pour assurer le respect des obligations résultant du présent article.

Article 109 Durée et fin des mandats

Les membres de la Commission sont désignés pour un mandat de cinq ans, renouvelable une fois.

Les membres de la Commission sont inamovibles pendant la durée de leur mandat. Sauf démission, il ne peut être mis fin aux fonctions de membre de la Commission dans les conditions définies dans le règlement intérieur de la Commission qu'en cas d'empêchement constaté par le bureau de la Commission ou en cas de perte de la qualité au titre de laquelle le membre concerné a été désigné.

Article 110 Vacance

En cas de vacance, il est procédé au remplacement du membre de la Commission vacant conformément aux dispositions du présent chapitre pour la durée de son mandat qui reste à courir.

Article 111 Immunité et indépendance

Les membres de la Commission ne reçoivent d'instruction d'aucune personne ou autorité.

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

Article 112 Indemnités

Les membres de la Commission perçoivent un traitement et des indemnités pour l'exercice de leurs fonctions au sein de la Commission, fixés par décret pris en Conseil des ministres.

Les frais engagés par les membres de la Commission pour assister aux réunions de la Commission et exécuter les attributions qui leur sont confiées sont remboursés.

Article 113 Serment des membres et agents de la Commission

Avant leur entrée en fonction, les membres et les agents de la Commission prêtent le serment sur le Coran devant la Cour d'appel : « Je jure solennellement de bien et fidèlement remplir mes fonctions au sein de la Commission Nationale de Protection des Données à Caractère Personnel, en toute indépendance, impartialité et équité et de façon digne et loyale, de respecter en toute circonstance les obligations que m'imposent ces fonctions et de garder le secret des délibérations ».

Section 3 : Fonctionnement de la Commission

Article 114 Personnel

La Commission peut pourvoir au recrutement de personnels administratifs. Elle dispose de services, dirigés par le président et placés sous son autorité.

Les agents de la Commission sont nommés par le président.

Article 115 Secret professionnel

Les membres et les agents de la Commission sont tenus au secret professionnel pour les faits, actes ou informations dont ils ont pu avoir connaissance dans le cadre ou à l'occasion de l'exercice de leurs fonctions, sous réserve de ce qui est nécessaire à l'établissement du rapport annuel de la Commission, y compris après la cessation de leurs fonctions.

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

Article 116 Établissement d'un règlement intérieur

Le règlement intérieur de la Commission est approuvé par voie réglementaire. Celui-ci fixe les règles particulières de son organisation et de son fonctionnement conformément au présent livre et notamment les modalités selon lesquelles les dossiers sont instruits et présentés à la Commission et les conditions dans lesquelles elle prend ses décisions et délibère.

Article 117 Autonomie de gestion

La Commission jouit de l'autonomie de gestion. Le budget de la Commission est préparé le président et adopté par la Commission. Le budget de la Commission est rendu public.

Le président de la Commission est ordonnateur des recettes et des dépenses. Un agent comptable est placé auprès de la Commission par le Ministre chargé du budget.

Article 118 Ressources financières

La Commission dispose d'un budget autonome nécessaire à l'accomplissement de ses missions, constitué par les crédits inscrits au budget de l'État. La Commission ne reçoit de don ou de subvention autre que de l'État. La Commission peut bénéficier de ressources propres issues de l'exercice de ses activités.

Les comptes de la Commission sont vérifiés annuellement par la Cour des Comptes et soumis au contrôle des organes de contrôles de l'État.

Article 119 Publicité des décisions

La Commission tient à la disposition du public ses avis, décisions ou recommandations et en assure dans la mesure du possible la publication sur son site Internet.

Article 120 Rapport annuel

La Commission présente chaque année au Président de la République, au président de l'Assemblée Nationale et au Président de la Commission Nationale des Droits de l'Homme (CNDH) un rapport public rendant compte de l'exécution de sa mission. Ce rapport est publié par la Commission sur son site Internet.

Chapitre 2 : Délégué à la protection des données à caractère personnel

Article 121 Statut et fonction

Le délégué à la protection des données à caractère personnel est une personne désignée afin d'assurer, d'une manière indépendante, le respect par le responsable de traitement et le sous-traitant des obligations mises à sa charge par le présent livre. Le délégué à la protection des données à caractère personnel peut exécuter d'autres missions et tâches. Le responsable de traitement et le sous-traitant veillent à ce que ces missions et tâches n'entraînent pas de conflit d'intérêts.

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

Il est soumis au secret professionnel ou à une obligation de confidentialité selon son statut en ce qui concerne l'exercice de ses missions.

Le délégué à la protection des données àcaractère personnel fait directement rapport au niveau le plus élevé de la direction du responsable de traitement ou du sous-traitant. Le responsable de traitement et le sous-traitant veillent à ce que le délégué à la protection des données à caractère personnel soit associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel. Le responsable de traitement et le sous-traitant aident le délégué à la protection des données à caractère à exercer ses missions en fournissant les ressources nécessaires ainsi que l'accès aux données à caractère personnel et aux opérations de traitement, et en lui permettant d'entretenir ses connaissances.

Le délégué à la protection des données à caractère personnel ne peut faire l'objet d'aucune sanction ou être relevé de ses fonctions par le responsable de traitement ou le sous-traitant du fait de l'accomplissement de ses missions.

Il peut saisir la Commission des difficultés qu'il rencontre dans l'exercice de ses missions.

Article 122 Missions

Les missions du délégué à la protection des données à caractère personnel sont les suivantes :

1) informer et conseiller le responsable de traitement ou le sous-traitant ainsi que leurs employés qui procèdent au traitement de données à caractère personnel sur les obligations qui leur incombent en vertu des dispositions du présent livre en matière de protection des données à caractère personnel ;

2) contrôler le respect par le responsable de traitement ou le sous-traitant des dispositions du présent livre en matière de protection des données à caractère personnel et des règles internes mises en place à cet effet, y compris s'agissant de la répartition des responsabilités, la sensibilisation et la formation du personnel participant aux opérations de traitement ainsi que des audits s'y rapportant ;

3) coopérer avec la Commission et notamment faire office de point focal pour la Commission sur les questions relatives au traitement de données à caractère personnel et mener des consultations sur tout autre sujet.

Le délégué à la protection des données à caractère personnel tient dûment compte, dans l'accomplissement de ses missions, du risque associé aux opérations de traitement compte tenu de la nature, de la portée, du contexte et des finalités du traitement.

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

Les personnes concernées peuvent prendre contact avec le délégué à la protection des données à caractère personnel au sujet de toutes les questions relatives au traitement des données les concernant et à l'exercice des droits que leur confèrent les dispositions du présent livre.

Article 123 Désignation

Le responsable de traitement et le sous-traitant désignent un délégué à la protection des données à caractère personnel lorsque :

1) le traitement est effectué par une autorité publique ou un organisme public, à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle ;

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

3) les activités principales du responsable de traitement ou du sous-traitant consistent e un traitement à grande échelle de catégories particulières de données à caractère personnel visée à l'Article 62 ou relatives à des condamnations pénales et infractions visées à l'Article 63 .

Dans les autres cas, le responsable de traitement ou le sous-traitant peuvent désigner un délégué à la protection des données à caractère personnel. Le délégué à la protection des données peut agir pour ces associations et autres organismes représentant des responsables du traitement ou des sous-traitants.

Le délégué à la protection des données à caractère personnel est désigné sur la base de ses qualités professionnelles et en particulier de ses connaissances spécifiques du droit et des pratiques en matière de protection des données à caractère personnel et doit bénéficier des qualifications requises pour exercer ses missions.

Un groupe d'entreprises peut désigner un seul délégué à la protection des données à caractère personnel à condition qu'un délégué soit facilement joignable à partir de chaque lieu d'établissement. Lorsque le responsable de traitement ou le sous-traitant est une autorité publique ou un organisme public, un seul délégué à la protection des données à caractère personnel peut être désigné pour plusieurs autorités ou organismes de ce type, compte tenu de leur structure organisationnelle et de leur taille.

La désignation du délégué à la protection des données à caractère personnel est notifiée à la Commission, avec ses coordonnées. Elle est portée, le cas échéant, à la connaissance des instances représentatives du personnel. Les coordonnées du délégué sont publiées par le responsable de traitement et le sous-traitant.

Article 124 Révocation

En cas de manquement constaté à ses devoirs, le délégué est déchargé de ses fonctions sur demande, ou après consultation, de la Commission.

Chapitre 3 : Registre national des traitements de données à caractère personnel

Article 125 Tenue du registre par la Commission

La Commission tient et met à la disposition du public un registre national des traitements automatisés de données à caractère personnel ayant fait l'objet d'une des formalités prévues à la Section 1 du Chapitre 2 du Titre 3 du présent livre, à l'exception de ceux mentionnés au dernier alinéa de l'Article 71 qui ont été dispensés de la publication de l'acte réglementaire qui les autorise.

Article 126 Contenu du registre

Le registre contient les informations suivantes sur chaque traitement :

1) l'acte autorisant la création

2) du traitement ou la date de la déclaration du traitement le cas échéant ;

3) la dénomination et la finalité du traitement ;

4) l'identité et l'adresse du responsable de traitement ou, si celui-ci n'est pas établi sur le territoire de la République de Djibouti, celles de son représentant ;

5) la fonction de la personne ou le service auprès duquel peuvent être exercés les droits de la personne concernée conformément au Chapitre 2 du Titre 2 du présent livre et ses coordonnées ;

6) les catégories de données à caractère personnel faisant l'objet du traitement ;

7) les destinataires et catégories de destinataires habilités à recevoir communication de ces données ;

8) le cas échéant, les transferts de données à caractère personnel envisagés à destination d'un pays tiers, société étrangère ou d'une organisation internationale.

Chapitre 4 : Contrôle de la mise en œuvre des traitements de données à caractère personnel

Article 127 Habilitation des agents

La Commission peut, par décision particulière, charger un ou plusieurs de ses membres ou agents de ses services de procéder à des contrôles et des vérifications portant sur tout traitement de données à caractère personnel, et, le cas échéant, d'obtenir des copies de tout document ou support d'information utile à sa mission.

Ceux des agents de la Commission qui peuvent être appelés à participer à la mise en œuvre des missions de contrôle en application du présent chapitre doivent y être habilités par la Commission. Cette habilitation ne dispense pas de l'application des dispositions définissant les procédures autorisant l'accès aux secrets protégés par la loi et assurant la protection des libertés individuelles.

Article 128 Droit de visite, perquisitions

Les membres de la Commission ainsi que ses agents habilités ont accès, dans les conditions prévues par le code de procédure pénale, pour l'exercice de leurs missions, aux lieux, locaux, enceintes, installations ou établissements servant à la mise en œuvre d'un traitement de données à caractère personnel et qui sont à usage professionnel, à l'exclusion des parties de ceux-ci affectées à un usage d'habitation.

Le procureur de la République en est préalablement informé.

En cas d'opposition du responsable des lieux, ou lorsqu'il s'agit de lieux mentionnés au premier alinéa affectés à un usage d'habitation, la visite ne peut se dérouler qu'avec l'autorisation du président du Tribunal de Première Instance ou du juge délégué par lui. Toutefois, lorsque l'urgence, la gravité des faits à l'origine du contrôle ou le risque de destruction ou de dissimulation de documents le justifie, la visite peut avoir lieu sans que le responsable des locaux en ait été informé, sur autorisation préalable du président du Tribunal de Première Instance. Dans ce cas, le responsable des lieux ne peut s'opposer à la visite. La visite s'effectue sous l'autorité et le contrôle du président du Tribunal de Première Instance ou du juge délégué par lui, en présence de l'occupant des lieux ou de son représentant qui peut se faire assister d'un conseil de son choix ou, à défaut, en présence de deux témoins qui ne sont pas placés sous l'autorité des personnes chargées de procéder au contrôle.

Le président du Tribunal de Première Instance est saisi à la requête du président de la Commission. Il statue par ordonnance motivée dans les conditions prévues par la loi. L'ordonnance est exécutoire au seul vu de la minute. Elle mentionne que le juge ayant autorisé la visite peut être saisi à tout moment d'une demande de suspension ou d'arrêt de cette visite et indique les voies et délais de recours.

Article 129 Droit de communication, enquêtes

Les membres de la Commission et ses agents habilités 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 utiles. Ils peuvent accéder aux programmes informatiques et aux données, demander la transcription de tout traitement dans des documents appropriés directement utilisables pour les besoins du contrôle. Ils peuvent être assistés par des experts choisis par la Commission.

Le secret ne peut leur être opposé sauf concernant les informations couvertes par le secret professionnel applicable aux relations entre un avocat et son client et par le secret des sources des traitements à des fins de journalisme. Le secret médical est également opposable s'agissant des informations qui figurent dans un traitement nécessaire aux fins de la médecine préventive, de la recherche médicale, des diagnostics médicaux, de l'administration de soins ou de traitements, ou de la gestion de service de santé. Dans ce cas, la communication des données médicales individuelles incluses dans cette catégorie de traitement ne peut se faire que sous l'autorité et en présence d'un médecin.

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

Pour le contrôle de services de communication au public en ligne, les membres de la Commission et ses agents habilités peuvent réaliser toute opération en ligne nécessaire à leur mission sous une identité d'emprunt. À peine de nullité, leurs actes ne peuvent constituer une incitation à commettre une infraction. L'utilisation d'une identité d'emprunt est sans incidence sur la régularité des constatations effectuées.

Article 130 Établissement de procès-verbaux

Il est dressé contradictoirement procès-verbal des contrôles, vérifications et visites effectuées par les membres et agents habilités de la Commission conformément aux dispositions du présent chapitre.

Article 131 Exception pour les traitements intéressant la sûreté de l'État, la défense ou la sécurité publique

Par dérogation, pour les traitements intéressant la sûreté de l'État, la défense ou la sécurité publique qu'un décret pris en Conseil des ministres a dispensé de la publication de l'acte réglementaire qui les autorise conformément aux dispositions de l'Article 71 , ce même décret peut également prévoir que le traitement n'est pas soumis aux dispositions du présent chapitre. Ce décret peut prévoir les conditions dérogatoires dans lesquelles la Commission peut procéder à des contrôles.

Chapitre 5 : Mesures correctrices et sanctions

Article 132 Compétence territoriale

La Commission peut prononcer les mesures prévues par le présent chapitre à l'égard des traitements de données à caractère personnel dont les opérations sont mises en œuvre, en tout ou partie, sur le territoire national, y compris lorsque le responsable de traitement ou le sous-traitant n'est pas établi sur le territoire de la République de Djibouti.

Article 133 Coopération internationale

La Commission peut, à la demande d'une autorité de contrôle exerçant des compétences analogues aux siennes dans un autre pays, procéder à des vérifications dans les mêmes conditions et selon les mêmes procédures que celles prévues au présent chapitre, sauf s'il s'agit d'un traitement de données à caractère personnel mentionné aux Article 70,Article 71 et Article 72.

La Commission est habilitée à communiquer les informations qu'elle recueille ou qu'elle détient, à leur demande, aux autorités de contrôle exerçant des compétences analogues aux siennes dans un autre pays.

Article 134 Avertissements et mises en demeure

La Commission peut adresser un avertissement au responsable de traitement concerné lorsqu'elle considère qu'un traitement de données à caractère personnel est susceptible de violer les dispositions du présent livre. Cet avertissement n'a pas le caractère d'une sanction.

Lorsqu'elle constate des manquements aux dispositions du présent livre, la Commission peut mettre en demeure le responsable de traitement de remédier aux manquements constatés dans le délai qu'elle fixe, notamment de satisfaire les demandes présentées par une personne concernée, y compris de rectifier ou d'effacer des données à caractère personnel et de notifier à la personne concernée les mesures prises pour satisfaire sa demande, de mettre un traitement en conformité avec les dispositions applicables, ou de communiquer une atteinte à la sécurité des données à caractère personnel. En cas d'urgence, ce délai peut être fixé à quarante-huit (48) heures. Si le responsable de

traitement se conforme à la mise en demeure qui lui est adressée, la Commission prononce la clôture de la procédure.

Article 135 Sanctions

Lorsque le responsable de traitement concerné ne se conforme pas à la mise en demeure qui lui a été adressée, la Commission peut, dans le respect du principe du contradictoire, prononcer à son encontre une ou plusieurs des sanctions suivantes :

1) une injonction de mettre en conformité le traitement de données à caractère personnel avec les dispositions du présent livre ou de satisfaire les demandes présentées par la personne concernée en vue d'exercer ses droits, qui peut être assortie, sauf dans des cas où le traitement est mis en œuvre par l'État, d'une astreinte dont le montant ne peut excéder 35.000.000 DJF par jour de retard à compter de la date fixée par la Commission ;

2) une injonction de cesser le traitement de données à caractère personnel si celui-ci relève du régime de la déclaration préalable ou de la déclaration préalable simplifiée ou s'il est dispensé de formalités préalables, ou le retrait de l'autorisation accordée par la Commission ;

3) le verrouillage de certaines données à caractère personnel ;

4) sauf dans le cas où le traitement est mis en œuvre par l'État, une sanction pécuniaire dont le montant est proportionné à la gravité des manquements commis et aux avantages tirés de ce manquement et ne peut excéder 70.000.000 DJF ou, s'agissant d'une entreprise, à 5% du chiffre d'affaires mondial hors taxe du dernier exercice clos, le montant le plus élevé étant retenu.

Toute sanction prononcée par la Commission peut être assortie d'une injonction de procéder dans un délai qu'elle fixe à toute modification ou suppression utile dans le fonctionnement des traitements de données à caractère personnel qui font l'objet de la sanction.

Les sanctions sont prononcées sur la base d'un rapport établi par la Commission. Ce rapport est notifié au responsable de traitement ou au sous-traitant concerné, qui peut présenter des observations et qui peut se faire représenter ou assister. La Commission peut entendre toute personne dont l'audition lui paraît susceptible de contribuer utilement à son information. Les personnes appelées soit à donner les renseignements à la Commission soit à témoigner devant elle sont déliées en tant que de besoin de leur obligation de discrétion.

L'astreinte est liquidée par la Commission, qui en fixe le montant définitif.

Lorsque la Commission 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 le montant de la sanction pécuniaire s'impute sur celui de l'amende qu'il prononce.

Le montant des sanctions pécuniaires est recouvré selon les règles de recouvrement des créances de l'État.

Article 136 Mesures conservatoires

Lorsqu'elle constate qu'un traitement de données à caractère personnel est mis en œuvre en l'absence de formalités préalables prescrites par le présent livre, la Commission peut prendre, sans préjudice des sanctions administratives et pénales prévues par le présent chapitre et le Chapitre 6 du Titre 4 du présent livre, les mesures nécessaires pour faire cesser le traitement, notamment :

1) faire apposer par un huissier de justice, aux frais du responsable de traitement, des scellés sur tout appareil, équipement ou local ayant servi ou contribué au traitement ;

2) faire procéder, en présence d'un huissier de justice, au démontage et à l'enlèvement de tels appareils et équipements et en assurer la garde ;

3) ordonner au responsable de traitement de rendre, à ses frais, inaccessible les moyens permettant le traitement.

Article 137 Mesures d'urgence

En cas d'urgence, lorsque la mise en œuvre d'un traitement de données à caractère personnel ou l'exploitation des données à caractère personnel traitées entraîne une violation de libertés et droits fondamentaux des personnes physiques, de libertés individuelles ou de la vie privée, la Commission peut, après une procédure contradictoire, engager une procédure d'urgence et :

1) ordonner l'interruption de la mise en œuvre du traitement pour une durée maximale de trois mois ;

2) prononcer un avertissement ;

3) ordonner le verrouillage de certaines données à caractère personnel traitées pour une durée maximale de trois mois ;

4) ordonner la mise en conformité du traitement, assortie, sauf dans le cas où le traitement est mis en œuvre par l'État, d'une astreinte dont le montant ne peut excéder 14.000.000 DJF par jour.

L'astreinte est liquidée par la Commission, qui en fixe le montant définitif.

En cas d'atteinte grave et immédiate aux libertés et droits fondamentaux des personnes physiques, aux libertés individuelles ou à la vie privée, la président de la Commission peut demander à la juridiction compétente d'ordonner, le cas échéant sous astreinte, toute mesure de sécurité nécessaire à la sauvegarde de ces libertés et droits.

Article 138 Notification et publicité des décisions

Les décisions prises par la Commission sont motivées et notifiées au responsable de traitement ou au sous-traitant concerné.

La Commission rend publics les avertissements, mises en demeures et sanctions qu'elle prononce. Elle peut également ordonner leur publication par le responsable de traitement à ses frais dans les journaux, publications et supports qu'elle désigne. La clôture d'une procédure fait l'objet de la même mesure de publicité, le cas échéant, que la mise en demeure.

Article 139 Recours contre les décisions de la Commission

Les décisions de la Commission ont le caractère d'actes administratifs et sont susceptibles de recours devant le Tribunal Administratif de Première Instance.

Chapitre 6 : Dispositions pénales

Article 140 Application du Code pénal

Les infractions établies par le présent chapitre sont réprimées dans les conditions prévues par le Code pénal, notamment s'agissant de la répression de la tentative, de la complicité, du recel et pour la condamnation des personnes morales, et pour les peines complémentaires pouvant être prononcées par le juge pénal.

Article 141 Non-respect des formalités préalables

Le fait, y compris par négligence, de procéder ou de faire procéder à un traitement de données à caractère personnel sans qu'aient été respectées les formalités préalables à sa mise en œuvre prévues par le Chapitre 2 du Titre 3 du présent livre est puni de 5 à 10 ans d'emprisonnement et de 7.000.000 DJF à 35.000.000 DJF d'amende, ou l'une de ces deux peines seulement.

Article 142 Non-respect des injonctions, mesures conservatoires ou mesures d'urgence

Le fait, y compris par négligence, de procéder ou de faire procéder à un traitement de données à caractère personnel en violation d'une décision prise par la Commission en application des dispositions du Chapitre 5 du présent titre est puni de 5 à 10 ans

d'emprisonnement et de 7.000.000 DJF à 35.000.000 DJF d'amende, ou l'une de ces deux peines seulement.

Article 143 Entrave à l'exercice par la Commission de ses prérogatives

Est puni d'une peine de 6 mois à 10 ans d'emprisonnement et de 7.000.000 DJF à 35.000.000 DJF d'amende le fait d'entraver l'exercice par la Commission de ses prérogatives soit en :

1) s'opposant à l'exercice des missions confiées à ses membres ou à ses agents habilités ;

2) refusant de communiquer à ses membres ou à ses agents habilités les renseignements et documents utiles à leur mission, ou en dissimulant lesdits documents ou renseignements, ou en les faisant disparaître ;

3) 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.

Article 144 Traitement non autorisé du numéro national d'identification

Le fait, hors les cas où le traitement a été autorisé dans les conditions prévues par le Chapitre 2 du Titre 3 du présent livre, de procéder ou faire procéder à un traitement de données à caractère personnel incluant parmi les données sur lesquelles il porte le numéro national d'identification de personnes physiques inscrit au registre national des personnes physiques est puni de 5 ans d'emprisonnement et de 4.000.000 DJF d'amende.

Article 145 Traitement illicite de données sensibles et de données relatives aux infractions

Le fait, hors les cas prévus par la loi, de mettre ou de conserver en mémoire informatisée, sans le consentement exprès de l'intéressé, des données à caractère personnel qui, directement ou indirectement, font apparaître ses origines raciales ou ethniques, ses opinions politiques, philosophiques ou religieuses ou son appartenance syndicale ou qui sont relatives à sa santé, est puni de 5 à 10 ans d'emprisonnement et de 7.000.000 DJF à 35.000.000 DJF d'amende.

Est puni des mêmes peines le fait, hors les cas prévus par la loi, de mettre ou de conserver en mémoire informatisée des données à caractère personnel concernant des infractions, des condamnations ou des mesures de sûreté.

Les dispositions du présent article sont applicables aux traitements non automatisés de données à caractère personnel dont la mise en œuvre ne se limite pas à l'exercice d'activités exclusivement personnelles.

Article 146 Traitement illicite de données de santé

En cas de traitement de données à caractère personnel ayant pour fin la recherche dans le domaine de la santé, est puni de 5 à 10 ans d'emprisonnement et de 7.000.000 DJF à 35.000.000 DJF d'amende le fait de procéder à un traitement :

1) sans avoir préalablement informé individuellement les personnes concernées du fait que des données à caractère personnel les concernant sont recueillies ou transmises, de leur droit d'accès, de rectification et d'opposition, de la nature des données transmises et des destinataires de celles-ci ;

2) malgré l'opposition de la personne concernée ou, lorsqu'il est prévu par la loi, en l'absence du consentement éclairé et exprès de la personne concernée, ou s'il s'agit d'une personne décédée, malgré le refus exprimé par celle-ci de son vivant.

Article 147 Collecte frauduleuse de données à caractère personnel

Le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite est puni de maximum 10 ans d'emprisonnement et de 7.000.000 DJF à 35.000.000 DJF d'amende.

Article 148 Détournement de finalité

Le fait, par toute personne détentrice de données à caractère personnel à l'occasion de leur enregistrement, de leur classement, de leur transmission ou de toute autre forme de traitement, de détourner ces informations de leur finalité telle que définie par la disposition législative, l'acte réglementaire ou la décision de la Commission autorisant le traitement automatisé ou par la déclaration préalable à la mise en œuvre de ce traitement, est puni d'une peine de 5 à 10 ans d'emprisonnement et de 7.000.000 DJF à 35.000.000 DJF d'amende.

Article 149 Transfert non autorisée de données à caractère personnel

Le fait de procéder ou de faire procéder à un transfert de données à caractère personnel faisant l'objet ou destinées à faire l'objet d'un traitement vers un pays tiers ou une organisation internationale en violation des dispositions du Chapitre 4 du Titre 3 est puni de 5 à 10 ans d'emprisonnement et de 8.000.000 DJF d'amende.

Article 150 Non-respect du droit d'opposition

Le fait de procéder à un traitement de données à caractère personnel concernant une personne physique malgré l'opposition de cette personne, lorsque ce traitement répond à des fins de prospection, notamment commerciale, ou lorsque cette opposition est fondée sur des motifs légitimes, est puni de 6 mois à 10 ans d'emprisonnement et de 7.000.000 DJF à 35.000.000 DJF d'amende.

Article 151 Non-respect des mesures de confidentialité et de sécurité

Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites par les Article 11Article 12 etArticle 13 est puni de 10 ans d'emprisonnement et de 8.000.000 DJF d'amende.

Article 152 Absence de notification des atteintes à la sécurité des données à caractère personnel

Le fait pour un responsable de traitement de ne pas procéder à la notification d'une atteinte à la sécurité de données à caractère personnel à la Commission ou à la personne concernée ou pour un sous-traitant de ne pas notifier cette atteinte au responsable de traitement conformément à l'Article 14 est puni de 5 à 10 ans d'emprisonnement et de 7.000.000 DJF à 35.000.000 DJF d'amende.

Article 153 Non-respect de la durée légale de conservation, traitement de données conservées au-delà de la durée légale de conservation

Le fait de conserver des données à caractère personnel au-delà de la durée prévue par la loi ou le règlement, par la demande d'autorisation ou d'avis, ou par la déclaration préalable adressée à la Commission, est puni de 5 à 10 ans d'emprisonnement et de 7.000.000 DJF à 35.000.000 DJF d'amende, sauf si cette conservation est effectuée à des fins historiques, statistiques ou scientifiques dans les conditions prévues par le présent livre.

Est puni des mêmes peines le fait, hors les cas prévus par le présent livre, de traiter à des fins autres qu'historiques, statistiques ou scientifiques des données à caractère personnel conservées au-delà de la durée mentionnée au premier alinéa.

Article 154 Divulgation non-autorisée de données à caractère personnel

Le fait, par toute personne qui a recueilli, à l'occasion de leur enregistrement, de leur classement, de leur transmission ou d'une autre forme de traitement, des données à caractère personnel dont la divulgation aurait pour effet de porter atteinte à la considération de la personne concernée ou à l'intimité de sa vie privée, de porter, sans autorisation de la personne concernée, ces données à la connaissance d'un tiers qui n'a pas qualité pour les recevoir est puni de 5 à 10 ans d'emprisonnement et de 7.000.000 DJF à 35.000.000 DJF d'amende.

La divulgation prévue à l'alinéa précédent est punie de 5 ans d'emprisonnement et de 7.000.000 DJF d'amende lorsqu'elle a été commise par imprudence ou négligence.

Dans les cas prévus aux deux alinéas précédents, la poursuite ne peut être exercée que sur plainte de la victime, de son représentant légal ou de ses ayants droit.

Article 155 Effacement des données à caractère personnel

Dans les cas prévus au présent chapitre, l'effacement de tout ou partie des données à caractère personnel faisant l'objet du traitement ayant donné lieu à l'infraction peut être ordonné par le juge. Les membres et les agents de la Commission sont habilités à constater l'effacement de ces données.

Article 156 Information par le procureur de la République et participation aux procédures

Le procureur de la République avise le président de la Commission des poursuites engagées relatives aux infractions au présent livre et des suites qui leur sont données.

Il l'informe de la date et de l'objet de l'audience de jugement par lettre recommandée adressée au moins dix (10) jours avant cette date. La juridiction d'instruction ou de jugement peut appeler le président de la Commission ou son représentant à déposer ses observations ou à les développer oralement à l'audience.

Livre Deuxième : Communications électroniques

Titre 1 Dispositions Générales

Chapitre premier : Dispositions préliminaires

Article 157 Champ d'application et exclusions

Le présent livre régit les activités de communications électroniques conduites par toute personne physique ou morale établissant et/ou exploitant un réseau de communications électroniques ou fournissant des services de communications électroniques sur le territoire de la République de Djibouti, quel que soit son statut juridique, sa nationalité, celle des détenteurs de son capital social ou de ses dirigeants, le lieu de son siège social ou de son établissement principal.

Sont exclus du champ d'application du présent livre :

1. les installations de l'État établies pour les besoins de la défense nationale ou de la sécurité publique, sauf en ce qui concerne les dispositions du Chapitre 2 du Titre 6 du présent livre, auxquelles celles-ci restent soumises ;

2. les activités relatives aux contenus des services destinés aux services de radiodiffusion télévisuelle et sonore, sauf en ce qui concerne les dispositions du Chapitre 2 du Titre 6 du présent livre, auxquelles celles-ci restent soumises ;

3. la fourniture de contenu sur des réseaux de communications électroniques ou l'exercice d'une responsabilité éditoriale sur ce contenu ;

4. les services de la société de l'information et, en particulier, le commerce électronique, la communication par voie électronique et les services de communication au public en ligne, à l'exclusion des services qui consistent entièrement ou principalement en la transmission de signaux sur des réseaux de communications électroniques.

Article 158 Objectifs

Le présent livre a notamment pour objectifs de :

5. définir les conditions générales d'établissement et d'exploitation des réseaux de communications électroniques et de fourniture de services de communications électroniques ;

6. définir le cadre et les modalités de régulation des activités liées aux communications électroniques ;

7. définir les conditions permettant de développer et moderniser les réseaux de communications électroniques et de fournir des services de communications électroniques de qualité à un coût accessible, permettant de préserver les marges de manœuvres nécessaires aux investissements futurs ;

8. encourager les investissements dans les infrastructures et les services en garantissant un accès équitable aux ressources rares et permettre une concurrence loyale et saine lorsque la taille du marché le permet et qu'elle permet d'améliorer les services et d'engager les investissements de long terme ;

9. promouvoir le développement de l'utilisation des services de communications électroniques et la croissance de l'économie numérique ;

10. développer la couverture nationale et l'accessibilité des services de communications électroniques, y compris à travers le service universel ;

11. préserver l'intégrité des infrastructures essentielles et la souveraineté de la République de Djibouti en matière de réseaux et services numériques ;

12. favoriser la création d'emplois directs et indirects liés au secteur des communications électroniques.

Chapitre 2 : Principes généraux

Article 159 Obligation de pose de câbles de communications électroniques à très haut débit en fibre optique dans le cadre de travaux publics et de génie civil

En vue de développer le maillage du territoire et la densification des réseaux de communications électroniques, les travaux de construction d'immeubles, routes et autoroutes, voies ferrées, réseaux de transport et distribution d'électricité et d'eau et autres travaux de génie civil susceptible d'accueillir des câbles de communications électroniques à très haut débit en fibre optique réalisés sur le territoire de la République de Djibouti sont tenus d'inclure le déploiement de tels câbles soit de manière aérienne soit de manière souterraine aux frais du maître d'ouvrage dans les conditions définies par l'Article 165 et la loi en vigueur.

Les maîtres d'ouvrages des travaux visés à l'alinéa précédent précisent les obligations de déploiement de câbles de communications électroniques à très haut débit en fibre optique dans les cahiers des charges de leur maître d'œuvre et de leurs contractants le cas échéant.

Un arrêté conjoint sur proposition du Ministère en charge des communications électroniques et du Ministère en charge des travaux publics précise les modalités techniques d'application du présent article.

Article 160 Obligation de fibrage des immeubles

Tout immeuble neuf regroupant plusieurs logements ou locaux à usage professionnel doit être équipé de câbles de communications électroniques à très haut débit en fibre optique nécessaires à la desserte de chacun des logements ou locaux à usage professionnel par un réseau de communications électroniques ouvert au public.

Tout immeuble neuf et maison individuelle neuve ne comprenant qu'un seul logement ou qu'un seul local à usage professionnel doit être équipé de câbles de communications électroniques à très haut débit en fibre optique nécessaires à la desserte du logement ou du local à usage professionnel par un réseau de communications électroniques ouvert au public.

Tout immeuble existant regroupant plusieurs logements ou locaux à usage professionnel faisant l'objet de travaux soumis à un permis de construire doit être équipé, aux frais des propriétaires, lorsque le coût des travaux d'équipement ne paraît pas disproportionné par rapport au coût des travaux couverts par le permis de construire, de câbles de communications électroniques à très haut débit en fibre optique nécessaires à la desserte de chacun des logements ou locaux à usage professionnel par un réseau de communications électroniques ouvert au public.

Le Ministre chargé de l'urbanisme est chargé de l'application du présent article.

Article 161 Neutralité technologique

Le Ministèreen charge des communications électroniques et l'Autorité de régulation veillent au respect du principe de neutralité technologique, sous réserve de prescriptions impératives d'ordre public, de coordination internationale ou d'efficacité technologique. A cet effet, aucun type particulier d'équipement, de réseau ou de technologie ne peut être privilégié de manière injustifiée pour l'établissement et l'exploitation de réseaux de communications électroniques, la fourniture de services de communications électroniques et l'utilisation de fréquences radioélectriques.

Article 162 Non-discrimination des opérateurs et égalité de traitement

Les opérateurs et exploitants intervenant sur le même secteur d'activité sont soumis au même régime juridique. Ils exercent dans les mêmes conditions l'ensemble des droits et sont soumis aux mêmes obligations applicables dans le cadre de ce régime.

Article 163 Activités des représentations diplomatiques, institutions étrangères et organismes jouissant de la personnalité juridique de droit international

Les activités de communications électroniques menées sur le territoire national par les représentations diplomatiques, les institutions étrangères et les organismes jouissant de la personnalité juridique de droit international sont exercées conformément aux accords ratifiés par la République de Djibouti.

Les ambassades et consulats de pays étrangers ainsi que les missions diplomatiques et les visites d'Etat de hautes personnalités sont exemptes du paiement des droits d'utilisation du spectre, pour autant que la même exemption s'applique aux ambassades, consulats et missions de la république de Djibouti dans le pays hôte.

Cette exemption s'applique également à la correspondance officielle qui relève de la convention de Vienne sur les relations diplomatiques et qui passe par le Ministère des affaires étrangers de la Républiques de Djibouti

Ces activités sont soumises aux dispositions du présent livre sous réserve des stipulations contraires des accords internationaux ratifiés par la République de Djibouti.

Chapitre 3 : Obligations générales des opérateurs et exploitants d'infrastructures alternatives

Article 164 Respect des accords et conventions internationaux

Les opérateurs sont tenus de respecter les accords et conventions internationaux et régionaux en matière de communications électroniques applicables en République de Djibouti.

Article 165 Respect du droit applicable, aménagement du territoire, servitudes, environnement

Pour la réalisation des travaux nécessaires à l'exploitation et à l'extension de leurs réseaux, les opérateurs et exploitants d'infrastructures passives respectent l'ensemble des dispositions législatives et réglementaires en vigueur, notamment les prescriptions en matière d'aménagement du territoire, de servitudes et de protection de l'environnement.

Ils veillent notamment à éviter les duplications inutiles d'infrastructures passives portant atteinte à l'environnement.

Lorsque cela est possible techniquement et financièrement, ils sont tenus de privilégier l'enfouissement des câbles à leur déploiement aérien.

Article 166 Secret des correspondances

Sous réserve des dérogations prévues par la loi, les opérateurs ainsi que les membres de leur personnel respectent le secret des correspondances effectuées au moyen de leurs réseaux et/ou services et la confidentialité des données relatives au trafic y afférent. Le secret couvre le contenu de la correspondance, l'identité des correspondants ainsi que, le cas échéant, l'intitulé du message et les documents joints à la correspondance.

Ils garantissent également la neutralité de traitement de ces communications et correspondances au regard des messages transmis et des informations qui y sont liées.

Article 167 Accès aux numéros d'urgence et aux numéros verts

Les opérateurs qui fournissent un service téléphonique au public garantissent également un accès ininterrompu aux numéros d'urgence et aux numéros verts, conformément aux règles applicables et dans les conditions précisées par l'Autorité de régulation.

Les opérateurs permettent l'accès par les autorités judiciaires, les services de la police, les services d'incendie et de secours et les services d'aide médicale d'urgence agissant, dans le cadre de missions d'interventions de secours, à leur liste d'utilisateurs complète non expurgée et mise à jour.

Article 168 Permanence et continuité des services

Les opérateurs assurent, de manière permanente et continue, la fourniture des services de communications électroniques. La rupture de tout service est considérée par nature comme une faute grave au titre de laquelle l'opérateur fautif encoure les sanctions prévues par la loi.

Article 169 Sécurité et intégrité des réseaux de communications électroniques

Les opérateurs prennent toutes les mesures appropriées pour assurer l'intégrité de leurs réseaux et garantir la continuité des services fournis.

Les opérateurs prennent toutes les dispositions techniques et organisationnelles nécessaires pour assurer la sécurité de leur réseau et de leurs services à un niveau adapté au risque existant. En particulier, des mesures sont prises pour prévenir ou limiter les conséquences des atteintes à la sécurité pour les utilisateurs et les réseaux interconnectés.

Les opérateurs prennent les mesures utiles pour assurer la sécurité et l'intégrité des dispositifs intégrés aux équipements terminaux nécessaires à l'identification et à l'authentification des utilisateurs pour la fourniture de services de communications électroniques.

Les opérateurs se conforment aux prescriptions techniques en matière de sécurité édictées par l'Autorité nationaleen charge de la cybersécurité. Celui-ci peut se faire

communiquer à titre confidentiel les dispositions prises pour la sécurisation du réseau et procéder ou faire procéder par un tiers à un contrôle de la sécurité et de l'intégrité des réseaux des opérateurs et du respect par ces derniers des dispositions du présent article. A cette fin, les opérateurs sont tenus de fournir toute information nécessaire et de donner accès à leurs installations.

Les opérateurs informent leurs utilisateurs des services existants permettant, le cas échéant, de renforcer la sécurité des communications.

Lorsqu'il existe un risque particulier de violation de la sécurité de leurs réseaux, les opérateurs informent les utilisateurs dans les plus brefs délais de ce risque ainsi que de tout moyen éventuel d'y remédier et du coût que cela implique.

Dès qu'il en a connaissance, l'opérateur informe par courrier recommandé avec accusé de réception l'Autorité en charge de la cybersécurité et l'Autorité de régulation de toute atteinte à la sécurité ou perte d'intégrité ayant un impact significatif sur le fonctionnement de ses réseaux ou de ses services. Lorsque l'atteinte à la sécurité ou la perte d'intégrité résulte ou est susceptible de résulter d'une attaque informatique, l'opérateur en informe également l'Autorité nationale en charge de la cybersécurité.

Dès que l'opérateur a mené une analyse des causes et des conséquences des atteintes à la sécurité ou pertes d'intégrité, il en rend compte à l'Autorité nationale en charge de la cybersécurité et à l'Autorité de régulation.

Les administrations veillent à la confidentialité des informations qui leur sont communiquées. Toutefois, lorsqu'il est d'utilité publique de divulguer les faits, l'Autorité de régulation peut en informer le public ou demander à l'opérateur d'y procéder.

Article 170 Identification des utilisateurs

Les opérateurs procèdent à l'identification de tous les utilisateurs de leurs services de communications électroniques au moment de la souscription aux services qu'ils fournissent.

Les conditions dans lesquelles les opérateurs procèdent à l'identification des utilisateurs sont précisées par voie réglementaire.

Article 171 Identification de l'appelant

À sa demande, tout utilisateur peut, sauf pour une raison liée au fonctionnement des services d'urgence ou à la tranquillité de l'appelé, s'opposer à l'identification par ses correspondants de son numéro de téléphone.

Article 172 Lutte contre la fraude liée au trafic international

Les opérateurs prennent toutes les mesures appropriées pour s'assurer que leur réseau n'est pas utilisé à des fins illégales ou frauduleuses et veillent à ce que tout ou partie du trafic entrant ou sortant de la République de Djibouti par l'intermédiaire de leur réseau ne soit pas dissimulé de leur fait ou de celui de tiers :

- soit en valeur, par exemple en diminuant, par quelque moyen que ce soit, le volume de trafic international entrant ou sortant de leur réseau ;

- soit en nature, par exemple en dissimulant du trafic international sous forme de trafic national.

A cet effet, les opérateurs :

- sont tenus de conclure des accords écrits avec leurs distributeurs ainsi qu'avec les opérateurs nationaux et étrangers acheminant du trafic international entrant ou sortant pour leur compte ou celui de leurs utilisateurs ; l'Autorité de régulation peut préciser les dispositions que doivent impérativement contenir ces accords et en obtenir copie sur demande ;

- mettent en place des mécanismes de détection des comportements frauduleux sur leur réseau, notamment sur la base des données de trafic qu'ils analysent conformément aux standards de l'industrie, à l'aide des équipements et logiciels adéquats ;

- mettent en place un système permettant d'identifier les adresses IP collectant du trafic de voix sur IP alimentant des équipements utilisés afin de transformer du trafic international en trafic national à l'aide de cartes SIM ; et

- communiquent à l'Autorité de régulation et aux autorités judiciaires tout case de fraude lié au trafic international dont ils ont connaissance.

En cas de non-respect des dispositions du présent article, les opérateurs pourront être tenus responsables de toute fraude liée au trafic international dont la réalisation aura été possible en raison de leur manquement.

L'Autorité de régulation précise les conditions dans lesquelles les dispositions du présent article sont mises en œuvre.

Article 173 Gestion des terminaux volés

Les opérateurs sont tenus de mettre en œuvre les dispositifs techniques destinés à interdire l'accès à leur réseau aux équipements terminaux mobiles identifiés et qui leur ont été déclarés volés et d'empêcher les communications émises au moyen de tels

équipements terminaux mobiles sur leur réseau, à l'exception des communications à destination des numéros d'urgence. Ces équipements terminaux mobiles sont bloqués sans délai, dès la réception par l'opérateur concerné de la déclaration officielle de vol, transmise par les services de police.

L'autorité judiciaire peut demander aux opérateurs de déroger aux dispositions de l'alinéa précédent aux fins d'enquête et de poursuite d'infractions pénales.

Article 174 Réquisitions des autorités judiciaires

Les opérateurs de communications électroniques sont tenus de déférer aux réquisitions émises par les autorités judiciaires habilitées conformément aux dispositions du Code de procédure pénale et du Chapitre 10 du Titre 1 et des Chapitres 1, 2 et 3 du Titre 2 du Livre Sixième.

Article 175 Prévention et gestion des déchets électroniques

Tout opérateur, fabricant, importateur et distributeur d'équipements et installations électroniques et/ou radioélectriques et d'équipements terminaux sont astreints au respect des normes environnementales, sous peine des sanctions prévues par le code de l'environnement.

Un décret pris en conseil des ministres sur proposition du ministère en charge des communications électroniques précise les modalités de gestion et de traitement des déchets électroniques.

Titre 2 Dispositions institutionnelles

Chapitre unique : Missions de l'Etat et dispositif institutionnel régissant le secteur des communications électroniques

Article 176 Missions de l'Etat

La règlementation du secteur des communications électroniques est du ressort de l'Etat. A ce titre, l'Etat veille notamment à ce que :

- la réglementation nationale soit conforme aux conventions et accords internationaux et régionaux en matière de communications électroniques, et en particulier aux conventions, règlements et recommandations de l'Union internationale des télécommunications, l'Union Africaine des Télécommunications (UAT), de l'Union Africaine et de la Ligue Arabe ;

- les intérêts de la défense nationale et de la sécurité publique soient garantis ;

- le développement de l'économie numérique dispose des infrastructures et des services de communications électroniques appropriés.

L'Etat dispose de l'usage exclusif du spectre des fréquences radioélectriques, en assure la planification, le découpage en bandes de fréquences et le contrôle et en administre l'utilisation par les différents affectataires dans le respect des principes d'efficacité et de rationalité de l'utilisation des fréquences radioélectriques.

Article 177 : Prérogatives du ministère

Le ministère chargé du secteur des communications électroniques :

- définit et met en œuvre la politique nationale de développement du secteur des communications électroniques

- veille au développement d'un secteur performant des communications électroniques, en coordination notamment avec les politiques gouvernementales développées dans les autres secteurs d'infrastructures, tels que la distribution d'eau, la production et la distribution d'énergie et le déploiement de réseaux de transport ;

- prend des mesures pour encourager les investissements et l'innovation dans les réseaux de communications électroniques ;

- veille à créer un environnement favorable à la création de richesse et d'emplois dans le secteur des communications électroniques

- oriente et contribue à l'exercice des missions de l'Etat en matière de communications électroniques ;

- sur la recommandation de l'autorité de régulation, décide au lancement des appels à candidatures pour l'octroi de licences ;

- propose au conseil des ministres la délivrance, la suspension et le retrait des licences su proposition de l'autorité de régulation ;

- analyser les propositions d'adaptation du cadre juridique applicable au secteur des communications électroniques de l'Autorité de régulation, ainsi que ses contributions aux projets de textes législatifs et réglementaires relatifs au secteur des communications électroniques, et le cas échéant veille à leur adoption et à leur mise en œuvre ;

- veille à ce que les moyens de communications électroniques couvrent l'ensemble du territoire national et favorisent une large utilisation d'Internet, y compris par

tous les consommateurs y compris ceux à faible revenu, les consommateurs ruraux et ceux qui sont défavorisés ;

- assure la représentation de la République de Djibouti auprès des organisations intergouvernementales à caractère international ou régional spécialisées dans les questions relatives aux communications électroniques, et favorise la coopération internationale et régionale ;

- assure, avec l'appui de l'Autorité de régulation, la préparation et la négociation des conventions et accords internationaux et régionaux en matière de communications électroniques, et veille à la mise en œuvre des conventions auxquelles l'Etat de Djibouti est partie.

Article 178 Prérogatives de l'Autorité de régulation

La régulation du secteur des communications électroniques est assurée par l'Autorité de régulation multisectorielle de Djibouti créée par la loi n° 74/AN/20/8ème L du 13 février 2020 portant création de l'Autorité de régulation multisectorielle de Djibouti.

En complément des missions générales qui lui sont confiées par l'article 5 de la loi n° 74/AN/20/8ème L du 13 février 2020, l'Autorité de régulation est chargée, conformément à l'article 6 de la même loi, des missions générales additionnelles suivantes dans le secteur des communications électroniques :

- veiller au respect des dispositions des textes législatifs et réglementaires régissant le secteur des communications électroniques de manière objective, transparente et non discriminatoire ;

- protéger les intérêts des utilisateurs et des opérateurs en prenant toute mesure propre à garantir l'exercice d'une concurrence loyale dans le secteur des communications électroniques ;

- accompagner le développement des réseaux et services de communications électroniques en favorisant les investissements et l'innovation dans le respect des standards internationaux et de leur évolution ;

- promouvoir la disponibilité et l'accessibilité des services des communications électroniques à tous les utilisateurs sur l'ensemble du territoire national ;

- participer à la protection de l'environnement, de la santé et à l'aménagement du territoire ;

- suivre et contrôler la qualité de service dans le secteur des communications électroniques ;

- analyser l'opportunité, recommander et mettre en œuvre les procédures d'attribution des licences ;

- décider du lancement et mettre en œuvre les procédures d'attribution des autorisations, des droits d'utilisation de fréquences radioélectriques ressources de numérotation et agréments et recevoir les déclarations préalables ;

- préparer les cahiers des charges assortis aux licences et autorisations ;

- mettre en œuvre la stratégie de déploiement du service universel des communications électroniques ;

- définir les spécifications techniques et administratives d'agrément des équipements terminaux et des équipements et installations radioélectriques ;

- contrôler le respect, par les opérateurs et toutes autres personnes soumises aux dispositions du présent livre des obligations qui leur incombent ;

- assurer la planification, la gestion et le contrôle de l'utilisation des ressources rares, et l'exercice des missions complémentaires qui lui sont confiées par le titre 6 du présent livre ;

- veiller au respect de la neutralité technologique pour les réseaux et services de communications électroniques ;

- formuler des propositions d'adaptation du cadre juridique applicable au secteur des communications électroniques ;

- contribuer à l'élaboration des projets de textes législatifs et réglementaires relatifs au secteur des communications électroniques et participer à leur mise en œuvre ;

- participer, aux côtés du ministère chargé des communications électroniques , à la représentation de la République de Djibouti auprès des organisations intergouvernementales à caractère international ou régional traitant de questions relatives aux communications électroniques et de gestion du spectre radioélectrique lorsque sont examinées des questions relevant de ses missions, ainsi qu'aux travaux visant à faire évoluer la réglementation internationale des communications électroniques ;

- favoriser la coopération internationale et régionale entre autorités nationales de régulation et avec les organismes internationaux et régionaux compétents ;

- appuyer le Ministère chargé des communications électroniques à la préparation et la négociation des conventions et accords internationaux et régionaux en matière

de communications électroniques. L'Autorité de régulation peut exercer toute mission d'intérêt public que lui confie l'Etat et assure une mission de conseil au Président de la République et au gouvernement en matière de communications électroniques.

L'Autorité de régulation est consultée sur tous les projets de textes législatifs et réglementaires relatifs au secteur de communications électroniques ou qui sont de nature à avoir un impact sur ce secteur. L'Autorité de régulation peut être saisie par le gouvernement pour avis sur toute question intéressant le secteur des communications électroniques ou de nature à avoir un impact sur ce secteur qui relève de sa compétence.

Titre 3 Régime juridique des activités de communications électroniques

Chapitre premier : Dispositions générales

Article 179 Régimes juridiques applicables aux activités de communications électroniques

Les activités de communications électroniques s'exercent librement sous réserve des régimes juridiques et des conditions assorties prévus par le présent titre :

1. le régime de la licence ;
2. le régime de l'autorisation :
3. le régime de la déclaration ; et
4. le régime libre.

Ne peuvent souscrire à l'un de ces régimes et se livrer aux activités de communications électroniques concernées les personnes qui ont perdu le droit d'exercer cette activité du fait d'un retrait ou d'une suspension prononcée en application de l'Article 321.

Article 180 Agrément des équipements de communications électroniques

Les équipements de communications électroniques sont soumis à agrément dans les conditions fixées au Chapitre 6 du présent titre.

Article 181 Modification des droits des personnes assujetties aux différents régimes juridiques

Les droits des personnes assujetties aux différents régimes juridiques peuvent être précisés par voie règlementaire. Ils ne peuvent être modifiés que selon les procédures énoncées au second alinéa du présent article.

Avant de modifier les régimes, les procédures, les droits et les obligations attachés à l'exercice des activités de communications électroniques, l'Autorité de régulation consulte et recueille les avis des acteurs du secteur. Les modifications opérées ne sont pas rétroactives.

Article 182 Opérateurs non nationaux

Sous réserve des engagements souscrits par la République de Djibouti et comportant une clause de réciprocité applicable au secteur des communications électroniques, les licences, autorisations, déclarations et agréments visés par le présent titre ne peuvent être accordés qu'à des entreprises de droit djiboutien ou souscrits que par des entreprises de droit djiboutien.

Chapitre 2 : Régime de la licence

Article 183 Activités soumises à licence

L'établissement et l'exploitation de réseaux de communications électroniques ouverts au public et la fourniture de services de communications électroniquesqui nécessitent l'utilisation de ressources rares sont subordonnés à l'obtention d'une licence délivrée par l'Autorité de régulation, assortie d'un cahier des charges, à l'exception des activités relevant des régimes de l'autorisation, de la déclaration ou du régime libre.

Un décret pris en Conseil des ministres pour l'application du présent article détermine les activités et les ressources rares qui nécessitent l'obtention d'une licence.

Article 184 Modalités d'octroi des licences

Les licences sont octroyées au terme d'un appel public à candidatures selon la procédure définie par le présent article.

A la demande de candidats potentiels ou sur son initiative, l'Autorité de régulation procède à l'analyse de l'opportunité d'attribuer de nouvelles licences. Cette analyse porte notamment sur :

- la situation économique du secteur des communications électroniques ;

- la qualité, la diversité et le niveau de tarification des services de communications électroniques offerts sur le marché et de ceux qu'il est proposé ou envisagé de fournir dans le cadre des nouvelles licences ;

- la taille et le potentiel du marché des communications électroniques ou du segment de ce marché en cause ;

- l'opportunité d'introduire de nouvelles technologies ou de nouveaux services de communications électroniques ;

- la capacité des opérateurs existants à investir dans les réseaux et services de communications électroniques et notamment dans les nouvelles technologies ou le défaut d'investissements ou d'établissement de plans d'investissement appropriés par ceux-ci ;

- la nécessité d'assurer la protection de l'intérêt supérieur de l'Etat, la défense nationale ou la sécurité publique, la protection de l'environnement et de la santé publique ou la protection d'infrastructures stratégiques.

Lorsqu'elle considère que l'octroi d'une ou plusieurs licences est justifié, l'Autorité de régulation publie un rapport détaillant les conclusions de son analyse d'opportunité et le type de licence qu'elle envisage d'attribuer puis recommande le lancement des appels à candidature au ministère chargé des communications électroniques. Si le ministère chargé des communications électroniques décide du lancement des appels à candidature, l'Autorité de régulation prépare le dossier d'appel à candidatures.

Le dossier d'appel à candidatures contient notamment le règlement de l'appel à candidatures, les conditions de la licence et le cahier des charges qui y est associé.

L'Autorité de régulation met en œuvre la procédure de sélection et instruit les dossiers selon les modalités fixées dans le règlement de l'appel à candidatures. A l'issue de son instruction, l'Autorité recommande au ministère des communications électronique, qui propose au conseil des ministres,l'octroi d'une ou plusieurs licences à des attributaires provisoires ou la non attribution de licence si elle considère que l'appel à candidatures a été infructueux.

Les modalités d'attribution des licences sont précisées par voie réglementaire.

Article 185 Contenu du cahier des charges

Le cahier des charges fixe les conditions particulières d'établissement et d'exploitation du réseau de communications électroniques et de fourniture de services de communications électroniques, ainsi que les engagements du titulaire de la licence.

L'autorité Autorité de régulation détermine le contenu du cahier des charges, qui décrit notamment :

- les conditions de permanence, de qualité et de disponibilité des réseaux et des services et les modes d'accès à ceux-ci ;

- la nature et les caractéristiques des obligations de couverture des réseaux et des services et le calendrier de déploiement ;

- les normes et les spécifications des réseaux et des services ;

- les droits et obligations en matière d'interconnexion, d'accès et de partage d'infrastructures ;

- les obligations relatives à la fourniture du service universel ;

- les obligations relatives aux conditions tarifaires ;

- les obligations relatives à la relation avec les utilisateurs et au respect du principe d'égalité de traitement des utilisateurs ;

- les prescriptions exigées par la défense nationale et la sécurité publique ;

- les modalités de contribution aux missions générales de l'Etat ;

- les obligations en matière de tenue de comptabilité et de communication d'informations à l'Autorité de régulation ;

- les modalités de paiement de la contrepartie financière et des différentes contributions ;

- la durée de la licence, les conditions et la procédure de son renouvellement, de la modification de ses termes et de sa fin ;

- les modalités de règlement des litiges.

Article 186 Cession et modification des licences

Les licences sont attribuées à titre personnel et individuel.

Elles ne peuvent être modifiées ou cédées à un tiers qu'avec l'accord préalable de l'Autorité de régulation.

Le bénéficiaire de la cession doit respecter l'ensemble des dispositions de la licence.

Article 187 Licences octroyées à titre expérimental

L'Autorité de régulation peut octroyer des licences à titre expérimental en vue d'accompagner le développement d'une technologie ou d'un service innovant du point de vue technique ou commercial selon une procédure simplifiée définie par voie réglementaire.

Ces licences peuvent préciser qu'au titre de l'activité ou du service concerné, et pour une durée maximale de deux (2) ans à compter de leur entrée en vigueur, les droits et

obligations du titulaire attachés à l'attribution des licences sont aménagés ou qu'il n'est pas soumis à tout ou partie de ces obligations.

Elles peuvent être assorties d'obligations relatives à l'information des utilisateurs finals concernant le caractère expérimental de l'activité ou du service concerné, ainsi qu'aux modalités de mise en conformité, à l'issue de l'expérimentation, avec les obligations auxquelles il a été dérogé.

Article 188 Publication

Les licences sont publiées au Journal officiel.

Chapitre 3 : Régime de l'autorisation

Article 189 Activités soumises à autorisation

Sont soumises à autorisation délivrée par l'Autorité de régulation :

1. les activités d'opérateur d'infrastructures ;
2. les activités d'exploitant d'infrastructure passives ;
3. la fourniture de services d'accès à Internet ; et
4. toute autre activité dont il est décidé par décret pris en Conseil des ministres de ne pas la soumettre à licence, auquel cas les règles applicables à cette activité sont fixées par l'Autorité de régulation en accord avec les dispositions du présent livre et en particulier du présent chapitre.

Article 190 Modalités d'octroi des autorisations

Les autorisations sont octroyées par l'Autorité de régulation dans les conditions qu'elle détermine, notamment au terme d'un appel public à candidatures ou sur demande.

Lorsque l'Autorité de régulation décide d'octroyer les autorisations après appel public à candidatures, elle évalue, à la demande de candidats potentiels ou sur son initiative, de l'opportunité d'initier un appel à candidatures et d'octroyer une ou plusieurs autorisations au regard notamment de :

- la situation économique du secteur des communications électroniques ;
- la qualité, la diversité et le niveau de tarification des services de communications électroniques offerts sur le marché et de ceux qu'il est proposé ou envisagé de fournir dans le cadre des nouvelles licences ;

- la taille et le potentiel du marché des communications électroniques ou du segment de ce marché en cause ;

- l'opportunité d'introduire de nouvelles technologies ou de nouveaux services de communications électroniques ;

- la capacité des opérateurs et exploitants d'infrastructures passives existants à investir dans les réseaux et services de communications électroniques et les infrastructures passives et notamment dans les nouvelles technologies ou le défaut d'investissements ou d'établissement de plans d'investissement appropriés par ceux-ci ;

- la nécessité d'assurer la protection de l'intérêt supérieur de l'Etat, la défense nationale ou la sécurité publique, la protection de l'environnement et de la santé publique ou la protection d'infrastructures stratégiques.

Lorsque l'Autorité de régulation décide d'octroyer les autorisations sur demande, elle se prononce dans un délai ne dépassant pas deux mois à compter de la date de la demande. Ce délai peut être prorogé d'un (1) mois, notamment en raison de la complexité technique des activités objet de l'autorisation sollicitée. En cas de silence du conseil de régulation et à l'issue de ce délai, une nouvelle demande d'autorisation peut être introduite auprès du Directeur Général de l'Autorité de Régulation Multisectorielle de Djibouti. L'absence de réponse à cette seconde demande dans un délai d'un mois vaut acceptation de la demande Le refus doit être motivé et notifie. L'autorisation peut être refusée pour les motifs suivants :

- l'octroi de l'autorisation est susceptible de mettre en péril la situation économique du secteur des communications électroniques ;

- la viabilité économique et la rentabilité du projet du demandeur ne sont pas démontrés ;

- le projet est contraire à l'intérêt supérieur de l'Etat ;

- le projet ou les technologies envisagés pour établir le réseau de communications électroniques ou fournir les services de communications électroniques posent un risque pour la défense nationale ou la sécurité publique, pour l'environnement ou la santé publique, ou risqueraient de compromettre des infrastructures stratégiques.

L'autorisation est accordée pour une durée déterminée par l'Autorité de régulation dans la décision portant autorisation.

Article 191 Contenu du cahier des charges

Un cahier des charges fixe les conditions particulières de l'exercice des activités soumises à autorisation, ainsi que les engagements du titulaire de l'autorisation.

L'Autorité de régulation détermine le contenu du cahier des charges, qui décrit notamment :

- les conditions de permanence, de qualité et de disponibilité des réseaux et des services et les modes d'accès à ceux-ci ;

- le cas échéant, la nature et les caractéristiques des obligations de couverture des réseaux et des services et le calendrier de déploiement ;

- les normes et les spécifications des réseaux et des services ;

- les droits et obligations en matière d'interconnexion, d'accès et de partage d'infrastructures ;

- le cas échéant, les obligations relatives à la fourniture du service universel ;

- le cas échéant, les obligations relatives aux conditions tarifaires ;

- le cas échéant, les obligations relatives à la relation avec les utilisateurs et au respect du principe d'égalité de traitement des utilisateurs ;

- les prescriptions exigées par la défense nationale et la sécurité publique ;

- les modalités de contribution aux missions générales de l'Etat ;

- les obligations en matière de tenue de comptabilité et de communication d'informations à l'Autorité de régulation ;

- les modalités de paiement de la contrepartie financière et des différentes contributions ;

- la durée de la licence, les conditions et la procédure de son renouvellement, de la modification de ses termes et de sa fin ;

- les modalités de règlement des litiges.

Article 192 Cession et modification des autorisations

Les autorisations sont attribuées à titre personnel et individuel.

Elles ne peuvent être modifiées ou cédées à un tiers qu'avec l'autorisation préalable de l'Autorité de régulation.

Le bénéficiaire de la cession doit respecter l'ensemble des dispositions de l'autorisation.

Article 193 Autorisations octroyées à titre expérimental

L'Autorité de régulation peut octroyer des autorisations à titre expérimental en vue d'accompagner le développement d'une technologie ou d'un service innovant du point de vue technique ou commercial.

Ces autorisations peuvent préciser qu'au titre de l'activité ou du service concerné, et pour une durée maximale de deux ans à compter de leur entrée en vigueur, les droits et obligations du titulaire attaché à l'attribution des autorisations sont aménagés ou qu'il n'est pas soumis à tout ou partie de ces obligations.

Elles peuvent être assorties d'obligations relatives à l'information des utilisateurs finals concernant le caractère expérimental de l'activité ou du service concerné, ainsi qu'aux modalités de mise en conformité, à l'issue de l'expérimentation, avec les obligations auxquelles il a été dérogé.

Article 194 Publication

Les décisions de l'Autorité de régulation portant autorisation sont publiées sur son site Internet et notifiées à leur titulaire.

Chapitre 4 : Régime de la déclaration

Article 195 Activités soumises à déclaration

Sont exercés librement sous réserve de déclaration préalable à l'Autorité de régulation et du respect des dispositions du présent livre :

- la fourniture de services à valeur ajoutée ;

- l'établissement et l'exploitation de réseaux indépendants ;

- toute autre activité dont il est décidé par décret pris en Conseil des ministres de ne pas la soumettre à licence ou à autorisation, auquel cas les règles applicables à cette activité sont fixées par l'Autorité de régulation en accord avec les dispositions du présent livre et en particulier du présent chapitre.

Article 196 Modalités de déclaration

Les déclarations doivent être faites à l'Autorité de régulation avant le début des activités ou de la fourniture des services. Celle-ci émet un récépissé le jour du dépôt du dossier

complet. Dès la remise de ce récépissé, l'activité objet de la déclaration peut être exercée par le déclarant.

L'Autorité de régulation dispose d'un délai d'un (1) mois à partir de la date de remise du récépissé pour faire savoir si elle s'oppose à la déclaration. Au terme du délai, le silence de l'Autorité vaut non-opposition à la déclaration.

L'opposition ne peut être motivée que par des considérations liées aux exigences de la sécurité publique, de la défense nationale ainsi que du respect de la réglementation en vigueur.

L'Autorité de régulation définit les conditions et modalités de dépôt des déclarations et les frais y afférents.

Article 197 Modalités de déclaration et de fourniture des services à valeur ajoutée

La déclaration relative à des services à valeur ajoutée doit contenir en particulier les informations suivantes :

- les modalités d'ouverture du service ;
- la couverture géographique ;
- les conditions d'accès :
- la nature des prestations objet du service :
- les tarifs qui seront appliqués aux utilisateurs.

Le service à valeur ajoutée déclaré doit utiliser, sous forme de location, les capacités de transmission d'un ou de plusieurs réseaux de communications électroniques ouverts au public existants, sauf si le fournisseur de ce service détient lui-même les licences et autorisations nécessaires pour utiliser les capacités de transmission nécessaires pour fournir le service. La déclaration identifie les capacités de transmission que le déclarant a l'intention d'utiliser pour fournir le service à valeur ajoutée.

Article 198 Règles applicables aux réseaux indépendants

Les réseaux indépendants peuvent être établis et exploités par toute personne physique ou morale, sous réserve de ne pas perturber le fonctionnement technique des réseaux de communications électroniques existants.

L'Autorité de régulation précise les conditions dans lesquelles lesdits réseaux peuvent être, le cas échéant, connectés à un réseau de communications électroniques ouvert au

public et ce, sans permettre l'échange de communications entre personnes autres que celles auxquelles l'usage du réseau indépendant est réservé.

Les exploitants de réseaux indépendants ne peuvent en aucun cas vendre ou mettre à dispositions leurs capacités sur ces réseaux, sauf à ce que ces réseaux constituent également des infrastructures alternatives.

Article 199 Information de l'Autorité de régulation en cas de modification de l'activité soumise à déclaration

Toute personne exerçant des activités ou fournissant des services ayant fait l'objet d'une déclaration informe l'Autorité de régulation de toute modification dans les informations ayant dû être fournies lors de la déclaration en application du présent chapitre.

En cas de transfert de l'activité ayant fait l'objet d'une déclaration, le nouvel exploitant est tenu d'informer l'Autorité de régulation du transfert dans un délai de trente jours à compter de la date de transfert, sous peine de caducité de la déclaration.

Article 200 Publication

L'Autorité de régulation tient et publie sur son site Internet une liste des activités et services déclarés.

Chapitre 5 : Régime libre

Article 201 Activités pouvant être exercées librement

Sous réserve de leur conformité aux dispositions du présent livre, tout réseau de communications électroniques ou service de communications électroniques ne relevant pas des régimes juridiques prévus au présent titre peut être établi, exploité et/ou fourni librement.

L'Autorité de régulation peut fixer des conditions générales d'établissement, d'exploitation et/ou de fourniture en tant que de besoin.

En particulier, sous réserve de la conformité de leurs équipements, peuvent être établis et exploités librement les réseaux internes et les installations radioélectriques exclusivement composées d'appareils de faible puissance et de courte portée dont les catégories sont déterminées par l'Autorité de régulation.

Chapitre 6 : Agrément liés aux équipements de communications électroniques

Article 202 Objectifs de l'agrément

L'agrément des équipements de communications électroniques a pour objectifs de garantir le respect de exigences essentielles fixées dans l'intérêt général dans le but d'assurer la sécurité des utilisateurs et du personnel des exploitants, la protection des réseaux de communications électroniques et notamment des échanges d'informations de commande et de gestion qui y sont associées, l'interopérabilité des services, l'interopérabilité des équipements ainsi que la bonne utilisation du spectre radioélectrique.

Article 203 Régime des équipements et installations radioélectriques

Les équipements et installations radioélectriques ne peuvent être fabriqués pour le marché intérieur, importés, détenus en vue de la vente, mis en vente, distribués à titre gratuit ou onéreux, connectés à un réseau de communications électroniques ouvert au public ou faire l'objet de publicité que s'ils sont agréés au préalable par l'Autorité de régulation.

A l'exception des installations radioélectriques des titulaires de licence ou d'autorisation, l'agrément est exigé dans tous les cas pour les installations radioélectriques, qu'elles soient destinées ou non à être connectées à un réseau de communications électroniques ouvert au public.

Les équipements et installations radioélectriques doivent, à tout moment, demeurer conformes au modèle agréé.

Article 204 Régime des équipements terminaux

Les équipements terminaux destinés à être connectés à un réseau de communications électronique ouvert au public font l'objet d'un agrément délivré par l'Autorité de régulation ou d'un organisme désigné par elle.

Article 205 Régime des installateurs d'équipements et installations radioélectriques

L'activité d'installateurs d'équipements et installations radioélectriques est soumise à l'obtention d'un agrément délivré par l'Autorité de régulation.

Article 206 Modalités d'octroi des agréments

L'Autorité de régulation définit les conditions d'agrément des équipements et installations ainsi que des installateurs, en tenant compte de la nécessité de garantir, dans l'intérêt général :

- la sécurité des utilisateurs et du personnel des exploitants ;

- la protection des réseaux de communications électroniques ;

- la compatibilité de ces équipements avec d'une part, les réseaux de communications électroniques ouverts au public et, d'autre part, les autres équipements permettant d'accéder à un même service ;

13. la bonne utilisation du spectre radioélectrique.

L'agrément est délivré dans un délai ne dépassant pas deux (2) mois à compter de la réception de la demande complète. Le silence de l'Autorité de régulation au terme de ce délai vaut refus. Tout refus d'agrément est motivé.

L'Autorité de régulation peut également tenir compte d'agréments ou de certifications délivrés dans d'autres pays.

Chapitre 7 : Contreparties financières, contributions, frais et redevances

Article 207 Contrepartie financière liée à l'octroi des licences et autorisations

L'octroi des licences et autorisations est subordonné au paiement d'une contrepartie financière dont les modalités sont précisées par voie réglementaire.

Article 208 Contribution au service universel

Les opérateurs sont tenus de contribuer au service universel des communications électroniques dans les conditions fixées par l'Article 308.

Article 209 Contribution au titre de la recherche, de la formation et de la normalisation

Les opérateurs sont tenus de verser à l'Autorité de régulation une contribution au titre de la recherche, de la formation et de la normalisation en matière de communications électroniques, calculée par un pourcentage du chiffre d'affaires hors taxes des activités de communications électroniques réalisées, fixé par voie réglementaire.

Les contributions des opérateurs sont collectées par l'Autorité de régulation.

Article 210 Contribution au titre de l'aménagement numérique du territoire et du fonctionnement de l'Autorité de régulation

Les opérateurs sont tenus de verser à l'Autorité de régulation une contribution au titre de l'aménagement numérique du territoire et du fonctionnement de l'Autorité de régulation, calculée par un pourcentage du chiffre d'affaires hors taxes des activités de communications électroniques réalisées, fixé par décret.

Les contributions des opérateurs sont collectées par l'Autorité de régulation.

Article 211 Frais de dossiers et autres redevances

Le dépôt d'une déclaration et la délivrance d'un agrément sont soumis au paiement de frais de dossier dont le montant est fixé par voie réglementaire

Titre 4 Interconnexion et accès aux réseaux de communications électroniques

Chapitre premier : Dispositions générales applicables à toute forme d'interconnexion ou d'accès

Article 212 Droit et obligation d'interconnexion et d'accès international

Les opérateurs non nationaux bénéficient d'un droit d'accès et d'interconnexion limité aux réseaux, infrastructures et services couverts par le présent chapitre dans des conditions d'égalité de traitement définies par décret. Le Ministère en charge des communications électroniques et l'Autorité de régulation veillent à ce que les opérateurs non nationaux assurent aux opérateurs des droits comparables à ceux dont ils bénéficient en application du présent article. Sous la supervision et la coordination de l'Autorité de régulation, les opérateurs veillent à ce que les modalités de déploiement de leurs réseaux facilitent leur interconnexion avec les réseaux des opérateurs non nationaux intervenant dans les pays limitrophes.

Article 213 Droit et obligation d'interconnexion et d'accès

Les opérateurs bénéficient d'un droit d'interconnexion et d'accès aux réseaux de communications électroniques ouverts au public, y compris aux infrastructures passives et actives les constituant, aux infrastructures passives et aux infrastructures alternatives dans les conditions prévues au présent titre.

Tout opérateur bénéficiant d'un accès au réseau d'un autre opérateur peut revendre les capacités disponibles sur ce réseau auxquelles il a accès, y compris les capacités nationales et internationales à d'autres opérateurs ou à ses utilisateurs.

Article 214 Mise en œuvre urgente de l'interconnexion

Lorsque l'Autorité de régulation considère qu'il est urgent d'agir afin de préserver la concurrence et protéger les intérêts des utilisateurs, elle peut demander la mise en œuvre immédiate de l'interconnexion entre les réseaux des opérateurs concernés, dans l'attente de la conclusion d'une convention d'interconnexion conformément à l'Article 218.

Article 215 Obligation de faire droit aux demandes raisonnables d'interconnexion et d'accès

Les opérateurs font droit, dans des conditions objectives, transparentes et non discriminatoires, aux demandes d'interconnexion et d'accès des autres opérateurs, présentées en vue d'établir des réseaux de communications électroniques ouverts au public ou de fournir au public des services de communications électroniques.

Toute demande d'accès ou d'interconnexion ne peut être refusée que si elle est techniquement ou financièrement impossible à satisfaire.

Toute décision de refus d'accès ou d'interconnexion opposée par un opérateur doit être motivée. Elle est notifiée au demandeur et portée à la connaissance de l'Autorité de régulation, ainsi qu'à l'Autorité de régulation nationale du pays dans lequel est établi l'opérateur non national, le cas échéant.

Article 216 Fixation de conditions techniques et tarifaires de l'interconnexion et de l'accès par l'Autorité de régulation

L'Autorité de régulation peut fixer les conditions techniques et tarifaires de l'interconnexion et de l'accès aux infrastructures passives et/ou actives et aux infrastructures alternatives.

L'Autorité de régulation peut notamment décider que la fourniture de certaines prestations d'interconnexion et d'accès visées à l'alinéa précédent doivent être orientées vers les coûts ou doivent faire l'objet d'une publication dans un catalogue d'interconnexion et d'accès.

Article 217 Obligations imposées aux opérateurs contrôlant l'accès aux utilisateurs finals

Les opérateurs qui contrôlent l'accès aux utilisateurs finaux peuvent se voir imposer des obligations en vue d'assurer le bon fonctionnement et l'interconnexion de leurs réseaux ainsi que l'accès aux services fournis sur d'autres réseaux.

Article 218 Conventions d'interconnexion et d'accès

L'interconnexion et l'accès font l'objet d'une convention de droit privé entre les parties concernées. Cette convention détermine, dans le respect des dispositions du présent chapitre, les conditions techniques et financières relatives à ces prestations.

L'Autorité de régulation peut, soit d'office, soit à la demande d'une partie, fixer un terme pour la signature de la convention. À la demande des parties, l'Autorité de régulation peut également les assister dans les négociations des conventions d'interconnexion et d'accès.

Les conventions d'interconnexion et d'accès sont communiquées à l'Autorité de régulation dès leur signature pour information. Toute modification de ces conventions par les parties doit également être notifiée à l'Autorité de régulation pour information.

Lorsque cela est indispensable pour garantir le respect de la loyauté de la concurrence et l'égalité des conditions de concurrence, la non-discrimination entre opérateurs et/ou l'interopérabilité des réseaux et services, l'Autorité de régulation peut demander aux parties de modifier les conventions d'interconnexion et d'accès ou leurs modifications qui lui sont soumises dans un délai d'un mois suivant leur réception. Elle adresse alors aux parties ses demandes de modification dûment motivées. A défaut d'observations de l'Autorité de régulation dans le délai d'un (1) mois, la convention ou la modification de celle-ci est réputée approuvée.

Les parties disposent d'un délai d'un (1) mois, à compter de la demande de modification pour adapter la convention. A l'expiration de ce délai, la convention est réputée contenir les modifications demandées par l'Autorité de régulation.

Article 219 Cartographie des installations ouvertes à l'interconnexion et à l'accès

Sans préjudice des obligations spécifiques qui peuvent être imposées aux opérateurs ayant une puissance significative sur un marché conformément à la Section 2 du Chapitre 2 du Titre 5 du présent livre, les opérateurs, les exploitants d'infrastructures passives et les exploitants d'infrastructures alternatives communiquent à l'Autorité de régulation, dans les conditions et selon la périodicité et les formats prescrits par elle, l'ensemble des informations pertinentes relatives à leur réseau de communications électroniques, leurs infrastructures passives et actives, leurs infrastructures alternatives ou celles auxquelles ils ont accès et à toutes autres informations pertinentes exigées par l'Autorité de régulation.

La nature et les conditions dans lesquelles ces informations sont communiquées à l'Autorité de régulation sont fixées par décision de l'Autorité de régulation.

Sur la base de ces informations, l'Autorité de régulation élabore une base de données et une cartographie :

- des réseaux et infrastructures actives et passives des opérateurs ouverts à l'accès et à l'interconnexion et offrant la possibilité aux autres opérateurs de s'y colocaliser ;

- des infrastructures passives détenues par les exploitants d'infrastructures passives ;

- des infrastructures alternatives détenues par les exploitants d'infrastructures alternatives ;

- des infrastructures essentielles.

Article 220 Catalogues d'interconnexion et d'accès

Les opérateurs établissent annuellement et communiquent à l'Autorité de régulation un catalogue d'interconnexion et d'accès dans lequel figurent l'ensemble des offres techniques et tarifaires proposées au titre de l'interconnexion et de l'accès, y compris les prestations de colocalisation.

L'Autorité de régulation peut imposer des modifications aux offres figurant dans les catalogues d'interconnexion et d'accès. L'Autorité de régulation peut également imposer que les prestations visées au Chapitre 2 du présent titre soient incluses dans le catalogue d'interconnexion et d'accès d'un opérateur.

L'Autorité de régulation peut également imposer à tout exploitant d'infrastructures passives ou alternatives de publier un catalogue d'interconnexion et d'accès, en précisant les prestations et les dispositions qui doivent y figurer.

Les catalogues d'interconnexion et d'accès sont approuvés par l'Autorité de régulation et sont publiés sur les sites Internet des opérateurs et, le cas échéant, des exploitants d'infrastructures passives ou alternatives et de l'Autorité de régulation.

Les prestations et dispositions que doivent contenir les catalogues d'accès et d'interconnexion et leur niveau de détail, ainsi que les conditions d'approbation et de publication de ces catalogues, sont précisées par décret pris en Conseil des ministres sur proposition du ministre en charge des communications électroniques.

Chapitre 2 : Dispositions particulières applicables à certaines formes d'accès

Article 221 Dispositions préliminaires

Sans préjudice des dispositions générales du Chapitre 1 du présent titre qui demeurent applicables, certaines formes d'accès font l'objet de mesures particulières additionnelles fixées par le présent chapitre.

Article 222 Principe de non-thésaurisation et de non spéculation

Les ressources et/ou capacités issues d'infrastructures essentielles ne peuvent faire l'objet de thésaurisation ou de spéculation de la part des opérateurs qui les exploitent ou qui y ont accès.

Article 223 Encouragement du partage d'infrastructures et imposition d'obligations par l'Autorité de régulation

L'Autorité de régulation encourage le partage d'infrastructures passives et actives dans des conditions d'équité, de non-discrimination et d'égalité.

Lorsque le partage d'infrastructures est rendu nécessaire pour satisfaire aux objectifs de concurrence, d'aménagement du territoire, d'urbanisme ou de protection de l'environnement ou du patrimoine, l'Autorité de régulation peut imposer aux opérateurs des obligations de partage des infrastructures passives ou actives, qu'elles soient existantes ou à construire, notamment les poteaux, les fourreaux, les lignes établies dans les immeubles bâtis, les points hauts, particulièrement dans les zones peu denses afin de mutualiser les investissements d'infrastructures des opérateurs ainsi qu'aux endroits ou l'accès à de telles capacités est limité.

- Lorsqu'elle envisage d'imposer de telles obligations, l'Autorité de régulation prend en compte :

- la viabilité technique et économique de la mise en place d'infrastructures concurrentes aux infrastructures concernées et de leur duplication ;

- la viabilité technique et économique de l'utilisation partagée des infrastructures envisagée ;

- le degré de faisabilité technique du partage des infrastructures existantes compte tenu des capacités disponibles ; et

- l'investissement initial réalisé par le propriétaire des infrastructures, sans négliger les risques inhérents à l'investissement.

Article 224 Accès aux infrastructures passives et aux infrastructures alternatives

Les exploitants d'infrastructures alternatives peuvent mettre à la disposition des opérateurs la capacité excédentaire dont ils disposent après avoir déployé des infrastructures destinées à leurs propres besoins ainsi que les droits de passage sur le domaine public, les servitudes, les emprises et les points hauts dont ils disposent.

Sans préjudice du droit de propriété des tiers, les exploitants d'infrastructures passives et les exploitants d'infrastructures alternatives font droit aux demandes raisonnables d'accès

à leurs infrastructures émanant d'opérateurs. La demande d'accès indique de manière détaillée les infrastructures passives ou alternatives auxquelles l'accès est demandé et comprend un échéancier de déploiement précis du réseau de communications électroniques ouvert au public.

La demande d'accès ne peut être refusée que si le refus est fondé sur des critères objectifs, transparents et proportionnés, tels que :

- la capacité technique des infrastructures passives ou alternatives à accueillir des éléments du réseau de communications électroniques ouvert au public, en raison notamment du manque d'espace disponible, y compris pour des besoins futurs d'espace qui ont été démontrés de manière suffisante ;

- la sécurité nationale, la sécurité publique, la santé publique ou la sécurité des personnes ;

- l'intégrité et la sécurité du réseau ;

- les risques de perturbation grave du réseau d'accueil ;

- la disponibilité d'autres offres de gros d'accès à des infrastructures passives ou alternatives de l'exploitant, adaptées à l'établissement de réseaux de communications électroniques, auxquelles l'accès est offert selon des modalités et conditions équitables et raisonnables ;

- le cas échéant, les obligations issues de réglementations sectorielles ou particulières applicables à l'exploitant d'infrastructures alternatives.

L'exploitant d'infrastructures passives ou alternatives communique sa réponse au demandeur dans un délai maximal de deux mois à compter de la réception d'une demande complète et motive, le cas échéant, sa décision de refus.

En cas de refus d'accès ou en l'absence d'accord sur les modalités d'accès, y compris tarifaires, dans le délai prévu à l'alinéa précédent, l'Autorité de régulation peut être saisie du différend relatif à cet accès par l'opérateur demandeur d'accès ou par l'exploitant d'infrastructures passives ou alternatives et statue dans les conditions prévues au Chapitre 2 du Titre 9 du présent livre.

L'accès ne doit pas porter atteinte aux droits de passage que sont en droit d'obtenir les autres opérateurs.

L'accès est fourni selon des modalités et dans des conditions, y compris tarifaires, équitables et raisonnables.

Les recettes et les dépenses relatives à cette mise à disposition sont retracées au sein d'une comptabilité distincte de l'exploitant d'infrastructures alternatives.

Article 225 Dégroupage de la boucle locale et de la sous-boucle locale

L'Autorité de régulation veille à ce que, dans les conditions qu'elle détermine en fonction de l'évolution des marchés, des réseaux et des services de communications électroniques et sur la base d'une analyse de l'opportunité de mettre en œuvre le dégroupage de la boucle locale et de la sous-boucle locale :

- les opérateurs puissent accéder à la boucle locale d'autres opérateurs sur la base d'un calendrier prédéfini ;

- les opérateurs souhaitant accéder à la boucle locale d'autres opérateurs soient tenus, de par leur cahier des charges, à un déploiement minimal d'infrastructure ;

- les opérateurs de boucle locale fournissent aux autres opérateurs l'accès à leurs infrastructures ainsi que la possibilité de colocalisation physique dans leurs propres locaux ou virtuelle pour faciliter le dégroupage dans des conditions objectives, transparentes et non discriminatoires, voire en respectant le principe d'orientation des prix en fonction des coûts ;

- les prestations liées au dégroupage de la boucle locale soient incluses dans le catalogue d'interconnexion et d'accès des opérateurs de boucle locale.

Article 226 Lignes déployées dans les immeubles bâtis

Toute personne établissant ou ayant établi dans un immeuble bâti ou exploitant une ligne de communications électroniques à très haut débit en fibre optique permettant de desservir un utilisateur final fait droit aux demandes raisonnables d'accès à ladite ligne et aux moyens qui y sont associés émanant d'opérateurs présentées en vue de fournir des services de communications électroniques à cet utilisateur final.

L'accès est fourni dans des conditions transparentes et non discriminatoires en un point situé, sauf dans les cas définis par l'Autorité de régulation, hors des limites de propriété privée et permettant le raccordement effectif d'opérateurs tiers, à des conditions économiques, techniques et d'accessibilité raisonnables. Dans les cas définis par l'Autorité de régulation, l'accès peut consister en la mise à disposition d'installations et d'éléments de réseau spécifiques demandés par un opérateur antérieurement à l'équipement de l'immeuble en lignes de communications électroniques à très haut débit en fibre optique, moyennant la prise en charge d'une part équitable des coûts par cet opérateur.

Article 227 Itinérance nationale

Les opérateurs de réseaux de communications électroniques mobiles doivent faire droit, dans des conditions objectives, transparentes et non discriminatoires, aux demandes de prestations d'itinérance nationale qui leur sont présentées par d'autres opérateurs de réseaux de communications électroniques mobiles dans les zones les moins denses du territoire qui sont déterminées par l'Autorité de régulation.

Lorsqu'un nouvel opérateur de réseaux de communications électroniques mobiles intègre le marché, ou lorsque la mise en œuvre d'une prestation d'itinérance nationale est rendue nécessaire pour satisfaire aux objectifs de concurrence ou d'aménagement numérique du territoire ou de protection de l'environnement ou du patrimoine, l'Autorité de régulation peut imposer aux opérateurs de réseaux de communications électroniques mobiles de fournir une prestation d'itinérance nationale sur des zones définies ou sur l'ensemble du territoire national.

Lorsqu'elle envisage d'imposer la fourniture d'une prestation d'itinérance nationale à un opérateur, l'Autorité de régulation prend en compte :

- la viabilité technique et économique de l'utilisation partagée des infrastructures envisagée ;

- le degré de faisabilité technique du partage des infrastructures existantes compte tenu des capacités disponibles ; et

- l'investissement initial réalisé par le propriétaire des infrastructures, sans négliger les risques inhérents à l'investissement.

Article 228 Itinérance internationale

Les opérateurs de réseaux de communications électroniques mobiles établis en République de Djibouti sont libres de conclure des contrats d'itinérance avec des opérateurs étrangers en vue de la fourniture de services de communications électroniques à des utilisateurs de ces opérateurs étrangers lorsqu'ils sont sur le territoire de la République de Djibouti et de la fourniture de services de communications électroniques à leurs utilisateurs lors de leur déplacements à l'étranger par ces opérateurs étrangers.

L'Autorité de régulation peut :

- enquêter sur les prix d'itinérance pratiqués dans la région ;

- procéder à des consultations avec les acteurs concernés ;

- identifier les opérateurs pratiquant des tarifs abusifs ou se livrant à d'autres pratiques ayant un effet anticoncurrentiel sur le marché national ;

- imposer aux opérateurs de permettre aux utilisateurs de services prépayés de bénéficier du service d'itinérance ;

- imposer aux opérateurs d'informer clairement et de façon transparente et détaillée les clients des tarifs appliqués pour l'itinérance.

L'itinérance internationale sur le territoire de la République de Djibouti doit être limitée à des fins de déplacements temporaires et/ou périodiques sur le territoire. Les opérateurs sont tenus de prévenir l'utilisation anormale ou abusive de services d'itinérance internationale, notamment lorsque les utilisateurs ont leur résidence principale fixée en République de Djibouti.

Il est interdit de commercialiser des cartes SIM d'un opérateur étranger à destination d'utilisateurs situés sur le territoire de la République de Djibouti ou de distribuer de telles cartes SIM sur le territoire de la République de Djibouti.

Article 229 Accueil des opérateurs mobiles virtuels

Les opérateurs de réseaux de communications électroniques mobiles doivent faire droit, dans des conditions objectives, transparentes et non discriminatoires, aux demandes d'interconnexion et d'accès présentées par des opérateurs mobiles virtuels en vue de leur permettre de fournir des services de communications électroniques aux utilisateurs.

Article 230 Accès aux capacités des câbles sous-marins

Tout exploitant et/ou gestionnaire de câbles sous-marins en fibre optique et/ou de stations d'atterrissement de ces câbles sur le territoire national de la République de Djibouti, y compris les points d'atterrissement virtuel, est soumis aux obligations particulières d'accès suivantes :

- fournir à tout opérateur qui le demande un accès à sa station d'atterrissement de câble sous-marin ainsi que des prestations de colocalisation, y compris virtuelle ;

- fournir à tout opérateur qui le demande une prestation d'interconnexion avec les capacités internationales qu'il détient sur un câble sous-marin en fibre optique raccordé à la station d'atterrissement qu'il exploite ainsi qu'avec toutes les capacités détenues par des opérateurs tiers sur l'ensemble des câbles sous-marins en fibre optique connectés à la station ;

- fournir à tout opérateur qui le demande une prestation de liaison d'interconnexion entre le point de présence de l'opérateur situé sur le territoire national et la station d'atterrissement du câble ;

- permettre à tout exploitant et/ou gestionnaire de câble sous-marin en fibre optique qui le demande de faire atterrir son câble à ladite station ;

- inclure les conditions techniques et tarifaires de ces prestations dans son catalogue d'interconnexion et d'accès dans une section spécifique relative à l'accès aux capacités internationales sous-marines.

L'ensemble des prestations d'accès aux capacités sur les câbles sous-marins se fait dans des conditions équitables, transparentes et non discriminatoires.

Article 231 Accès aux points d'échange Internet

Toute personne exploitant un point d'échange Internet fait droit, dans des conditions objectives, transparentes et non discriminatoires, aux demandes raisonnables d'accès auxdits points d'échange présentées par des opérateurs de réseaux de communications électroniques dans les conditions fixées au Chapitre 1 du présent titre.

Titre 5 Promotion de la concurrence

Chapitre premier : Dispositions préliminaires

Section 1 : Dispositions générales

Article 232 Libre exercice des activités de communications électroniques et liberté de fixation des tarifs

Les opérateurs et exploitants d'infrastructures passives exercent librement leurs activités et fixent librement les tarifs de leurs services dans le respect des dispositions du présent livre ainsi que des conditions propres aux licences, autorisations et autorisations d'utilisation de fréquences radioélectriques qui leur sont octroyées.

Article 233 Concurrence loyale et absence de discrimination

L'exploitation des réseaux de communications électroniques ouverts au public, la fourniture de services de communications électroniques et la fourniture d'accès aux infrastructures passives s'effectuent dans des conditions transparentes et de concurrence loyale conformément à la législation en vigueur.

Les opérateurs fournissent leurs services de gros dans des conditions de transparence et de non-discrimination pour assurer un traitement équivalent des autres opérateurs à circonstances équivalentes. Les opérateurs sont tenus de fournir des services et de communiquer des informations aux autres opérateurs dans les mêmes conditions que celles assurées pour leurs propres services ou accordées à leurs filiales ou partenaires.

Article 234 Tenue d'une comptabilité analytique

Les opérateurs et exploitants d'infrastructures passives tiennent une comptabilité analytique permettant de déterminer les coûts, produits et résultats de chaque réseau exploité ou chaque service offert.

Leurs comptes et les états de synthèse, dégagés au plus tard dans les trois (3) mois suivant la date de clôture de l'exercice comptable, sont soumis annuellement pour audit, à leurs frais, à un organisme désigné par l'Autorité de régulation.

Ledit audit a pour objet de s'assurer que les états de synthèse présentés reflètent de manière régulière et sincère les coûts, produits et résultats de chaque réseau exploité ou de chaque service offert.

Article 235 Publication d'indicateurs

L'Autorité de régulation publie périodiquement des indicateurs et observatoires sur le taux de pénétration des réseaux de communications électroniques ouverts au public et des services de communications électroniques sur le territoire national notamment en fonction de la technologie et des services, la qualité de service, les parts de marchés des opérateurs sur les marchés de gros et de détail, les tarifs des services de détail, et tout autre indicateur jugé pertinent par l'Autorité de régulation.

Article 236 Saisine du Ministre chargé du commerce en cas de constat de pratiques restrictives de la concurrence ou de pratiques anticoncurrentielles dans le secteur des communications électroniques

L'Autorité de régulation saisit le Ministèreen charge du commerce des abus de position dominante et des pratiques entravant le libre exercice de la concurrence dont elle pourrait avoir connaissance dans le secteur des communications électroniques. Elle peut également le saisir pour avis sur toute autre question relevant de sa compétence.

Lorsque l'Autorité de régulation est saisie d'une demande relevant de la compétence du Ministère en charge du commerce en matière de concurrence, elle transmet le dossier à ce dernier.

Le Ministère en charge du commerce communique à l'Autorité de régulation toute saisine entrant dans le champ de compétence de celle-ci et recueille son avis sur les pratiques dont il est saisi dans le secteur des communications électroniques.

Section 2 : Dispositions modificatives

Article 237 Sanction des pratiques anticoncurrentielles

En complément de l'article L.2295-7 du code de commerce, les infractions prévues à l'article L.2294-2 du Code de commerce sont punies d'une amende proportionnée à la

gravité des faits reprochés, à l'importance du dommage causé à l'économie, à la situation de la personne sanctionnée ou du groupe auquel la personne appartient s'il s'agit d'une personne morale et à l'éventuelle réitération de pratiques prohibées par la section 2 du présent chapitre. Le montant de l'amende et déterminé individuellement pour chaque personne sanctionnée et motivé.

Si la personne sanctionnée n'est pas une entreprise, le montant maximum de la sanction est de vingt-cinq millions (25.000.000) de DJF. Si la personne sanctionnée est une entreprise, le montant maximum de la sanction est 10% du montant du chiffre d'affaires mondial hors taxes le plus élevé réalisé au cours d'un des exercices clos depuis l'exercice précédant celui au cours duquel les pratiques anticoncurrentielles ont été mises en œuvre. Si les comptes de l'entreprise concernée ont été consolidés ou combinés en vertu des textes applicables à sa forme sociale, le chiffre d'affaires pris en compte est celui figurant dans les comptes consolidés ou combinés de l'entreprise consolidant ou combinant.

La juridiction compétente peut également ordonner aux frais du condamné la publication intégrale ou par extraits de sa décision dans un ou plusieurs journaux qu'elle désigne et l'affichage dans les lieux qu'elle indique.

En outre, elle peut prescrire l'insertion du texte intégral de sa décision dans le rapport établi sur les opérations de l'exercice par le gérant ou le conseil d'administration.

Chapitre 2 : Régulation *ex ante* des opérateurs ayant une puissance significative sur un marché du secteur des communications électroniques

Section 1 : Cadre de la régulation ex ante

Article 238 Identification périodique des marchés pertinents et détermination des opérateurs ayant une puissance significative

L'Autorité de régulation détermine, au regard notamment des obstacles au développement d'une concurrence effective, les marchés pertinents du secteur des communications électroniques.

Après avoir analysé l'état et l'évolution prévisible de la concurrence sur ces marchés, l'Autorité de régulation établit la liste des opérateurs réputés posséder une puissance significative sur chacun de ces marchés qu'elle publie.

Cette liste est révisée par l'Autorité de régulation aussi souvent que nécessaire et au moins tous les trois (3) ans. Au moment de la révision de l'analyse d'un marché, l'Autorité de régulation publie un bilan relatif aux résultats effectifs, eu égard aux objectifs poursuivis, des mesures décidées en vertu de l'analyse précédente.

Article 239 Critères d'évaluation de la puissance d'un opérateur

Tout opérateur disposant, sur un marché pertinent de services ou d'un groupe de services, d'une puissance au moins équivalente à 25% du volume ou de la valeur de ce marché, peut être déclaré comme ayant une puissance significative.

La puissance de l'opérateur est appréciée sur la base des critères suivants :

- sa capacité à influencer le marché ;

- son chiffre d'affaires par rapport à la taille du marché ;

- le contrôle qu'il exerce sur les moyens d'accès à l'utilisateur final ;

- sa capacité à agir indépendamment de ses concurrents, de ses clients et des utilisateurs ;

- la présence et l'influence d'exploitants d'infrastructures passives sur le marché pertinent concerné.

Article 240 Détermination et modalités d'imposition d'obligations particulières aux opérateurs ayant une puissance significative sur un marché

L'Autorité de régulation fixe, en les motivant, les obligations imposées aux opérateurs ayant une puissance significative sur un marché du secteur des communications électroniques dans le but de garantir une concurrence saine.

Ces obligations s'appliquent pendant une durée limitée fixée par l'Autorité de régulation, pour autant qu'une nouvelle analyse du marché concerné effectuée en application de la présente section ne les rende pas caduques.

- Lorsqu'elle examine s'il y a lieu d'imposer un ou plusieurs obligations visées au présent chapitre, l'Autorité de régulation prend notamment en considération les éléments suivants :

- la viabilité technique et économique de l'utilisation ou de la mise en place d'infrastructures concurrentes, compte tenu du rythme auquel le marché évolue et de la nature et du type d'interconnexion et d'accès concerné, notamment la viabilité d'autres produits d'accès en amont ;

- le degré de faisabilité de la fourniture d'accès proposée, compte tenu de la capacité disponible ;

- l'investissement initial réalisé par le propriétaire des infrastructures, sans négliger les risques inhérents à l'investissement ;

- la nécessité de préserver la concurrence à long terme en apportant une attention particulière à la concurrence effective fondée sur les infrastructures ;

- le cas échéant, les éventuels droits de propriété intellectuelle.

L'Autorité de régulation n'impose d'obligations aux opérateurs ayant une puissance significative sur un marché du secteur des communications électroniques qu'en l'absence de concurrence effective et durable et les supprime dès lors qu'une telle concurrence existe.

Article 241 Typologie d'obligations pouvant être imposées aux opérateurs ayant une puissance significative sur un marché

L'Autorité de régulation peut imposer aux opérateurs ayant une puissance significative sur un marché du secteur des communications électroniques des obligations spécifiques :

- de transparence ;

- de non-discrimination ;

- de séparation comptable ;

- d'accès aux réseaux de communications électroniques, y compris aux infrastructures passives et aux infrastructures alternatives auxquels ces opérateurs ont eux-mêmes accès ;

- de contrôle des prix et d'obligations relatives au système de comptabilisation des coûts.

Le cas échéant, l'Autorité de régulation peut également imposer la mise en œuvre d'un mécanisme de sélection ou de présélection du transporteur. Dans ce cas, les modalités de mise en œuvre de cette mesure sont précisées par voie règlementaire.

Section 2 : Mise en œuvre des obligations particulières s'imposant aux opérateurs ayant une puissance significative

Article 242 Obligation de transparence

L'Autorité de régulation peut imposer des obligations de transparence concernant l'interconnexion et/ou l'accès en vertu desquelles les opérateurs doivent rendre publiques des informations bien définies, telles que les informations comptables, les spécifications techniques, les caractéristiques du réseau, les modalités et conditions de fourniture et d'utilisation et les prix.

Article 243 Obligation de non-discrimination

L'Autorité de régulation peut imposer des obligations de non-discrimination. Dans une telle hypothèse, l'Autorité de régulation peut notamment imposer que le catalogue d'interconnexion et d'accès que l'opérateur publie :

- soit suffisamment détaillée pour garantir que les bénéficiaires de ce catalogue ne sont pas tenus de payer pour des ressources qui ne sont pas nécessaires pour le service demandé ;

- comprenne une description des offres pertinentes réparties en divers éléments selon les besoins du marché ;

- soit accompagnée des modalités et conditions correspondantes, y compris des prix.

Article 244 Obligation de séparation comptable

L'Autorité de régulation peut imposer des obligations de séparation comptable en ce qui concerne certaines activités de communications électroniques.

Elle peut notamment obliger un opérateur à rendre ses prix de gros et ses prix de transferts internes transparents, entre autres pour garantir le respect de l'obligation de non-discrimination ou, en cas de nécessité, pour empêcher des subventions croisées abusives.

L'Autorité de régulation peut spécifier le format et les méthodologies comptables à utiliser.

Dans ce cas, la comptabilité de l'opérateur est auditée annuellement à ses frais par un organisme désigné par l'Autorité de régulation.

Article 245 Communication de documents comptables à l'Autorité de régulation

L'Autorité de régulation peut, afin de faciliter la vérification du respect des obligations de transparence, de non-discrimination et de séparation comptable, exiger que les documents comptables, y compris les données concernant les recettes provenant de tiers, lui soient fournis si elle en fait la demande.

L'Autorité de régulation peut publier ces informations dans la mesure où elles contribuent à l'instauration d'un marché ouvert et concurrentiel, dans le respect des dispositions régissant la confidentialité des informations commerciales.

Article 246 Obligation de faire droit à des demandes spécifiques d'accès

L'Autorité de régulation peut imposer aux opérateurs l'obligation de faire droit aux demandes raisonnables d'accès à des éléments spécifiques de leur réseau et à des ressources associées et d'en autoriser l'utilisation, notamment lorsqu'elle considère qu'un refus d'octroi de l'accès ou des modalités et conditions déraisonnables ayant un effet similaire empêcheraient l'émergence d'un marché de détail concurrentiel durable ou risqueraient d'être préjudiciables aux utilisateurs finals.

Les opérateurs peuvent notamment se voir imposer :

- de négocier de bonne foi avec les opérateurs qui demandent un accès ;

- d'interconnecter des réseaux ou des ressources de réseau ;

- de ne pas retirer l'accès aux ressources lorsqu'il a déjà été accordé ;

- de fournir une possibilité de colocalisation physique et virtuelle ou d'autres formes de partage des ressources, y compris le partage des gaines, des bâtiments ou entrées de bâtiment, des antennes ou pylônes, des trous de visite et regards et boîtiers situés dans la rue ;

- de donner accès à des services associés comme ceux relatifs à l'identité, l'emplacement et l'occupation ;

- d'accorder à des tiers l'accès à des éléments et/ou ressources de réseau spécifiques, y compris l'accès dégroupé à la boucle locale ;

- de fournir des prestations d'accès nécessaire aux opérateurs mobiles virtuels ;

- d'accorder un accès ouvert aux interfaces techniques, protocoles ou autres technologies clés qui revêtent une importance essentielle pour l'interopérabilité des services ou des services de réseaux mobiles virtuels ;

- de fournir des prestations d'itinérance nationale ;

- de fournir les services spécifiques nécessaires pour garantir aux utilisateurs l'interopérabilité des services de bout en bout, notamment en ce qui concerne les ressources destinées aux services de réseaux intelligents ou permettant l'itinérance sur les réseaux mobiles ;

- d'offrir des services de gros particuliers en vue de la revente à des tiers ;

- de fournir l'accès à des systèmes d'assistance opérationnelle ou à des systèmes logiciels similaires nécessaires pour garantir l'existence d'une concurrence loyale dans la fourniture des services.

L'Autorité de régulation peut associer à ces obligations des conditions concernant le caractère équitable ou raisonnable de ces prestations et le délai de fourniture de ces prestations.

Lorsque l'Autorité de régulation impose à un opérateur l'obligation de fournir un accès conformément aux dispositions du présent article, elle peut fixer, de façon objective, transparente, proportionnée et non discriminatoire, des conditions techniques ou opérationnelles auxquelles le fournisseur et/ou les bénéficiaires de l'accès doivent satisfaire pour assurer le fonctionnement normal du réseau.

Article 247 Obligations visant à empêcher les effets anticoncurrentiels de la structure tarifaire de détail

L'Autorité de régulation peut imposer aux opérateurs des obligations d'information et de nature tarifaire relatives à leurs offres et leurs tarifs de détail visant à empêcher ou limiter :

- toute différenciation tarifaire on-net / off-net ;

- tout effet de ciseau tarifaire ;

- tout effet d'éviction ;

- toute subvention croisée d'une activité de communications électroniques par une autre activité.

À cet effet, l'Autorité de régulation peut imposer aux opérateurs un contrôle *ex ante* de leurs offres et tarifs (y compris promotionnels) sur le marché de détail concerné.

Article 248 Obligation d'orientation des prix de gros en fonction des coûts, système de comptabilisation des coûts

L'Autorité de régulation peut imposer des obligations concernant l'orientation des prix de gros en fonction des coûts et des obligations concernant les systèmes de comptabilisation des coûts, pour la fourniture de types particuliers d'interconnexion et/ou d'accès, lorsqu'une analyse du marché indique que l'opérateur pourrait, en l'absence de concurrence efficace, maintenir les prix à un niveau excessivement élevé ou comprimer les prix.

L'Autorité de régulation tient compte des investissements réalisés par l'opérateur et lui permet une rémunération raisonnable du capital adéquat engagé, compte tenu des risques encourus.

Article 249 Asymétrie tarifaire

L'Autorité de régulation peut décider la fixation de tarifs asymétriques au bénéfice d'un nouvel opérateur qui intègre un marché, ou en cas de déséquilibre significatif des ressources en fréquences au détriment d'un opérateur. Une telle mesure doit être justifiée et doit être limitée dans le temps.

Article 250 Critères d'établissement des méthodologies comptables et tarification imposées

L'Autorité de régulation veille à ce que les méthodologies comptables et de tarification qui seraient imposées visent à :

- promouvoir l'efficacité économique ;

- favoriser une concurrence durable ; et

- optimiser les avantages pour l'utilisateur.

À cet égard, l'Autorité de régulation peut également prendre en compte les prix en vigueur sur les marchés concurrentiels comparables.

Article 251 Publicité et transparence des systèmes de comptabilisation des coûts

Lorsque la mise en place d'un système de comptabilisation des coûts est rendue obligatoire dans le cadre d'un contrôle des prix, l'Autorité de régulation veille à ce que soit mise à la disposition du public une description du système de comptabilisation des coûts faisant apparaître au moins les principales catégories au sein desquelles les coûts sont regroupés et les règles appliquées en matière de répartition des coûts.

Le respect du système de comptabilisation des coûts est vérifié par un organisme désigné par l'Autorité de régulation. Une attestation de conformité est publiée annuellement.

Article 252 Preuve du respect des obligations de nature tarifaire

Lorsqu'un opérateur est soumis à une obligation de nature tarifaire, notamment une obligation d'orientation des prix en fonction des coûts, c'est à lui qu'il incombe de prouver que ses tarifs sont déterminés en fonction des coûts, en tenant compte d'un retour sur investissements raisonnable.

Afin de calculer les coûts de la fourniture d'une prestation efficace, l'Autorité de régulation peut utiliser des méthodes de comptabilisation des coûts distinctes de celles appliquées par l'opérateur.

L'Autorité de régulation peut demander à un opérateur de justifier intégralement ses prix et, si nécessaire, en exiger l'adaptation.

Titre 6 Gestion des ressources rares

Chapitre premier : Dispositions générales

Article 253 Typologie des ressources rares

Au sens du présent livre, les ressources rares comprennent :

1. le spectre radioélectrique ;
2. les ressources de numérotation ; et
3. les noms du domaine Internet national « .dj ».

Article 254 Respect des conventions internationales

Les règles de gestion des ressources rares tiennent compte de de la politique nationale dans le secteur ainsi que des conventions et accords internationaux et régionaux ratifiés par la République de Djibouti en la matière.

Article 255 Retrait des droits d'utilisation de fréquences radioélectriques et de ressources de numérotation

En cas d'annulation, de retrait, d'abandon, d'expiration, ou de toute autre forme de perte de la licence, de l'autorisation ou de radiation de la déclaration nécessaire au support d'une activité de communications électroniques, les droits d'utilisation de fréquences radioélectriques assignées et de ressources de numérotation octroyés utilisés dans le cadre de cette activité conformément aux dispositions des Chapitres 2 et 3 du présent titre sont automatiquement retirés. Il en va de même en cas d'interdiction d'exercer cette activité de communications électroniques prononcée à l'encontre de la personne intéressée.

Chapitre 2 : Fréquences radioélectriques

Section 1 : Gestion du spectre radioélectrique

Article 256 Incorporation du spectre radioélectrique dans le domaine public de l'Etat

Le spectre radioélectrique fait partie du domaine public de l'Etat.

L'utilisation de fréquences radioélectriques disponibles sur le territoire de la République de Djibouti par les titulaires de droits d'utilisation de fréquences radioélectriques constitue un mode d'occupation privatif du domaine public de l'Etat.

Article 257 Attributions de l'Autorité de régulation s'agissant de la gestion du spectre radioélectrique

L'Autorité de régulation est chargée, pour le compte de l'Etat, de la planification, de la gestion et du contrôle de l'utilisation du spectre radioélectrique. Conformément aux textes en vigueur, elle gère le spectre radioélectrique selon des modalités favorisant la souplesse tout en restant conformes aux traités et accords internationaux et régionaux ratifiés par la République de Djibouti. A ce titre, elle :

- établit, en concertation avec l'ensemble des affectataires, un plan national d'attribution des fréquences radioélectriques ;

- tient à jour l'ensemble des documents relatifs à l'affectation et l'utilisation des fréquences radioélectriques ;

- définit les conditions d'utilisation des fréquences radioélectriques dont l'assignation lui est confiée ;

- coordonne les assignations de fréquences radioélectriques dans les bandes attribuées en partage et émet des avis sur les projets d'assignation dérogatoires de fréquences radioélectriques dans les bandes attribuées à titre exclusif ;

- procède à la notification des assignations nationales de fréquences radioélectriques au fichier international des fréquences de l'Union internationale des télécommunications dont elle est, pour ce domaine, l'interlocuteur unique ;

- assure la coordination internationale des fréquences radioélectriques aux frontières et de celle des systèmes de communications électroniques par satellites ;

- organise et assure le contrôle de l'utilisation des fréquences radioélectriques, sans préjudice des compétences de contrôles spécifiques exercés par les affectataires, et de traite les cas de brouillage qui lui sont soumis.

Elle veille à ce que tous les usagers de fréquences radioélectriques soient incités ou amenés à optimiser l'utilisation des fréquences ou des bandes de fréquences qu'ils exploitent.

Le rapport annuel public des activités de l'Autorité de régulation mentionné par les articles 19 et 21 de la loi n° 74/AN/20/8ème L du 13 février 2020 portant création de l'Autorité de régulation multisectorielle de Djibouti est rédigé inclut une présentation de l'état de la gestion du spectre radioélectrique et des actions y afférentes menées par celle-ci dans l'année écoulée.

Article 258 Coordination des utilisations du spectre radioélectrique avec les utilisateurs publics

L'Autorité de régulation coordonne l'utilisation du spectre radioélectrique et l'assignation des fréquences radioélectriques au niveau national en concertation avec les affectataires et leurs services.

Article 259 Attribution des fréquences radioélectriques et établissement du plan national d'attribution des fréquences

Dans le respect des traités et accords internationaux et régionaux ratifiés par la République de Djibouti, notamment en conformité avec les dispositions du Règlement des radiocommunications établies par l'Union internationale des télécommunications, l'Autorité de régulation établit et tient à jour un plan national d'attribution des fréquences radioélectriques.

Ce plan national répartit les bandes de fréquences du spectre radioélectrique entre les différentes catégories de services de radiocommunications identifiés par le Règlement des radiocommunications et les attribue aux affectataires pour que ceux-ci, le cas échéant, les assignent pour utilisation par leurs propres services pour leurs besoins propres ou les assignent pour utilisation à des tiers.

Le plan national d'attribution des fréquences radioélectriques est adopté sur proposition de l'Autorité de régulation par décret pris en Conseil des ministres.

Article 260 Assignation des fréquences radioélectriques et tenue des fichiers national et international des fréquences

L'Autorité de régulation assigne les fréquences radioélectriques qui lui sont attribuées et en autorise l'usage par l'octroi de droits d'utilisation de fréquences radioélectriques ou par l'intermédiaire de conditions générales d'utilisation.

L'assignation des fréquences radioélectriques attribuées aux services de radiodiffusion télévisuelle et sonore est effectuée par l'Autorité de régulation au profit des titulaires d'une autorisation d'exercice de ces activités délivrée par l'autorité compétente et pour la même durée.

L'assignation des fréquences radioélectriques pour les usages gouvernementaux dans les bandes de fréquences attribuées aux autres affectataires, notamment pour la défense nationale, la sécurité publique, la sécurité aérienne et la météorologie, est effectuée directement par les affectataires concernés selon les modalités qu'ils déterminent. L'utilisation de ces fréquences radioélectriques n'est pas soumise à l'octroi de droits d'utilisation de fréquences radioélectriques par l'Autorité de régulation.

L'Autorité de régulation établit et tient à jour l'ensemble des documents relatifs à l'emploi des fréquences radioélectriques. Les assignations de fréquences radioélectriques par l'ensemble des affectataires sont enregistrées par l'Autorité de régulation dans un fichier national des fréquences. A cet effet, les affectataires lui transmettent les informations nécessaires sous réserve de la protection du secret défense.

L'Autorité de régulation procède également à la notification des assignations nationales de fréquences radioélectriques au fichier international des fréquences de l'Union internationale des télécommunications.

Article 261 Optimisation de l'usage du spectre radioélectrique et réaménagement

L'Autorité de régulation mène des analyses prospectives du spectre des fréquences radioélectriques en vue de son utilisation optimale par les usagers publics ou privés, sans préjudice des compétences propres des affectataires.

Elle procède à l'examen périodique de l'utilisation du spectre et recommande les aménagements qui lui paraissent nécessaires et coordonne les réaménagements du spectre radioélectrique.

Les utilisateurs de fréquences radioélectriques supportent l'intégralité du coût des réaménagements nécessaires à la mise à disposition des fréquences qui leur sont assignées. Le préfinancement d'une partie de cette dépense peut être assuré par le fonds de réaménagement du spectre.

Ce fonds est géré par l'Autorité de régulation, qui est notamment chargée d'évaluer le coût des opérations de réaménagement du spectre des fréquences radioélectriques, d'en établir le calendrier de réalisation et de veiller à leur mise en œuvre.

Les modalités de création, d'organisation et de fonctionnement du fonds sont fixées par décret pris en Conseil des ministres sur proposition de la Présidence de la République.

Section 2 : Utilisation du spectre radioélectrique

Article 262 Fréquences radioélectriques dont l'utilisation est autorisée par décret pris en Conseil des ministres

L'utilisation des fréquences radioélectriques identifiées dans le décret prévu par l'Article 183 est autorisée par décret pris en Conseil des ministres et soumise aux conditions fixées par le cahier des charges accompagnant la licence et par l'Autorité de régulation.

Article 263 Fréquences radioélectriques dont l'utilisation est autorisée par l'Autorité de régulation

L'Autorité de régulation peut soumettre l'utilisation de fréquences radioélectriques qui lui sont attribuées à l'obtention de droits d'utilisation octroyés par elle lorsque cela est nécessaire pour :

- éviter les brouillages préjudiciables ;
- assurer la qualité technique des services de radiocommunications ;
- préserver l'efficacité de l'utilisation du spectre radioélectrique ;
- assurer la protection de l'environnement ou de la santé publique ;
- l'aménagement du territoire ; ou
- la promotion des investissements.

La décision d'octroi de droits d'utilisation détermine les conditions spécifiques d'utilisation des fréquences radioélectriques concernées.

Article 264 Modalités d'octroi des droits d'utilisation de fréquences radioélectriques

L'Autorité de régulation octroie les droits d'utilisation de fréquences radioélectriques sur demande dans des conditions objectives, transparentes et non discriminatoires en tenant compte des besoins d'aménagement du territoire.

Ces droits d'utilisation ne peuvent être refusés que pour l'un des motifs suivants :

- la sauvegarde de l'ordre public, les besoins de la défense nationale ou de la sécurité publique ;
- la bonne utilisation des fréquences radioélectriques ;

- l'incapacité technique ou financière du demandeur à faire face durablement aux obligations résultant des conditions d'exercice de son activité ;

- la condamnation du demandeur pour l'une des infractions mentionnées aux Article 334, Article 335, Article 336,Article 337 et Article 338.

Les délais d'octroi des droits d'utilisation de fréquences radioélectriques et de notification des conditions de leur renouvellement, ainsi que les obligations qui s'imposent aux titulaires pour permettre le contrôle par l'Autorité de régulation des conditions d'utilisation des fréquences radioélectriques sont fixés par décret pris en Conseil des ministres.

Article 265 Fréquences radioélectriques dont l'utilisation est libre

Les fréquences radioélectriques non spécifiquement assignées aux personnes les utilisant ou que l'Autorité de régulation ne soumet pas l'utilisation à l'octroi de droits d'utilisation peuvent être utilisées librement sous réserve du respect des conditions générales d'utilisation définies par décision de l'Autorité de régulation notamment afin de garantir la bonne utilisation du spectre radioélectrique.

Article 266 Conditions d'utilisation des fréquences radioélectriques

L'Autorité de régulation définit les conditions générales et spécifiques d'utilisation des fréquences ou bandes de fréquences radioélectriques qui lui sont attribuées et qui portent notamment sur :

- la nature et les caractéristiques techniques des équipements, réseaux et services qui peuvent utiliser les fréquences ou bandes de fréquences ;

- les conditions techniques nécessaires pour éviter les brouillages préjudiciables et pour limiter l'exposition du public aux champs électromagnétiques ;

- les obligations résultant d'accords internationaux ayant trait à l'utilisation des fréquences ;

- le cas échéant, les obligations spécifiques à l'utilisation expérimentale de fréquences ;

- pour les droit d'utilisation octroyés par l'Autorité de régulation, leur durée ainsi que le délai minimal dans lequel sont notifiés au titulaire les conditions de leur renouvellement et les motifs d'un refus de renouvellement ;

- pour les droit d'utilisation octroyés par l'Autorité de régulation, les redevances dues par le titulaire ;

- pour les droit d'utilisation octroyés par l'Autorité de régulation, les critères d'une utilisation effective des fréquences ou bandes de fréquences et le délai dans lequel le titulaire doit les utiliser sous peine d'une abrogation de ces droits.

Article 267 Cession et modification droit d'utilisation de fréquences radioélectriques

Les droit d'utilisation de fréquences radioélectriques sont attribuées à titre personnel et individuel.

Ils ne peuvent être modifiés ou cédés à un tiers qu'avec l'autorisation préalable de l'Autorité de régulation.

Le bénéficiaire de la cession doit respecter l'ensemble des conditions d'utilisation des fréquences radioélectriques fixées par l'Autorité de régulation.

Article 268 Droits d'utilisation de fréquences radioélectriques octroyés à titre expérimental

L'Autorité de régulation peut octroyer des droits d'utilisation de fréquences radioélectriques à titre expérimental en vue d'accompagner le développement d'une technologie ou d'un service innovant du point de vue technique ou commercial.

Ces droits d'utilisation peuvent préciser qu'au titre de l'activité ou du service concerné, et pour une durée maximale de deux ans à compter de leur entrée en vigueur, les droits et obligations du titulaire attachés à la délivrance des droits d'utilisation sont aménagés ou qu'il n'est pas soumis à tout ou partie de ces obligations.

Ils peuvent être assortis d'obligations relatives à l'information des utilisateurs finals concernant le caractère expérimental de l'activité ou du service concerné, ainsi qu'aux modalités de mise en conformité, à l'issue de l'expérimentation, avec les obligations auxquelles il a été dérogé.

Ils sont assortis de conditions techniques et opérationnelles nécessaires pour éviter les brouillages préjudiciables.

Article 269 Frais et redevances d'utilisation du spectre radioélectrique

L'octroi de droits d'utilisation de fréquences radioélectriques par l'Autorité de régulation fait l'objet de redevances pour l'occupation du domaine public de l'Etat qui en résulte. Les modalités de versement et le montant de ces redevances sont précisés par décret. Ces redevances sont recouvrées comme les créances de l'Etat relatives au domaine.

L'octroi de droits d'utilisation de fréquences radioélectriques fait l'objet de frais de gestion fixés par décret sur proposition de la Présidence de la République.

Article 270 Certificat d'opérateur radiotélégraphiste ou radiotéléphoniste et indicatifs internationaux

L'Autorité de régulation détermine les catégories d'installations radioélectriques d'émission pour la manipulation desquelles la possession d'un certificat d'opérateur radiotélégraphiste ou radiotéléphoniste est obligatoire et les conditions d'obtention de ce certificat, ainsi que les modalités d'attribution et de retrait des indicatifs des séries internationales utilisées par les stations radioélectriques autorisées en application du présent livre.

Section 3 : Contrôle de l'utilisation du spectre

Article 271 Règles de compatibilité électromagnétique et d'ingénierie du spectre

L'Autorité de régulation établit les règles de compatibilité électromagnétique, d'ingénierie du spectre ainsi que les normes propres à assurer une bonne utilisation des équipements, installations et réseaux radioélectriques, qui s'imposent à toute personne qui exploite des équipements, installations et réseaux radioélectriques.

Article 272 Implantation, transfert et modification des stations radioélectriques

Afin d'assurer la meilleure utilisation des sites disponibles, ainsi que la prévention des brouillages préjudiciables entre usagers du spectre radioélectrique, l'Autorité de régulation coordonne l'implantation sur le territoire national des stations radioélectriques de toute nature.

A cet effet, l'implantation de certaines catégories de stations radioélectriques ne peut être faite qu'avec son accord. L'accord de l'Autorité de régulation est également nécessaire en cas de modification des implantations ou de transfert des stations radioélectriques soumises à accord.

Un décret pris en Conseil des ministres définit les catégories de stations radioélectriques pour lesquelles, en raison de leurs caractéristiques techniques, et en particulier de leur puissance d'émission, cet accord n'est pas requis ou si un simple avis est requis. En particulier, sous réserve du respect des dispositions du présent livre et des conditions fixées par l'Autorité de régulation, l'implantation des stations radioélectriques exclusivement composées d'appareils de faible puissance et de courte portée n'est pas soumise à son accord.

En liaison avec les autres affectataires, l'Autorité de régulation établit et diffuse les documents, répertoires et fichiers relatifs aux stations radioélectriques et aux zones de groupement des stations radioélectriques.

Article 273 Contrôle de l'utilisation des fréquences radioélectriques et des stations radioélectriques de toutes catégories

L'Autorité de régulation exerce un contrôle permanent sur l'utilisation des fréquences radioélectriques ainsi que les conditions d'exploitation des stations radioélectriques de toutes catégories.

Article 274 Prévention et traitement des brouillages préjudiciables

L'Autorité de régulation assure la prévention et le traitement des brouillages préjudiciables. L'Autorité de régulation assure les fonctions de bureau centralisateur prévues par le Règlement des radiocommunications afin de coordonner la remédiation aux brouillages et interférences des émissions et réceptions radioélectriques.

Dans le cas où une perturbation d'un système radioélectrique lui est signalée, l'Autorité de régulation étudie cette perturbation et, le cas échéant, formule des préconisations aux personnes utilisant les fréquences radioélectriques concernées dans le but de faire cesser la perturbation.

Lorsque les préconisations formulées par l'Autorité de régulation ne sont pas respectées, elle peut suspendre l'accord donné pour l'implantation de la station radioélectrique en cause ou enjoindre la cessation des émissions radioélectriques lorsque l'implantation de la station radioélectrique en cause n'était pas soumise à son accord et en informe l'affectataire concerné sans délai.

L'exploitation d'une station radioélectrique en l'absence d'accord de l'Autorité de régulation ou lorsque cet accord a été suspendu ou lorsque l'Autorité a enjoint de cesser les émissions radioélectriques engage la responsabilité civile et pénale de l'exploitant de cette station radioélectrique.

Article 275 Protection du public par rapport aux champs électromagnétiques

L'exploitation de réseaux de communications électroniques, d'équipements, d'installations et de réseaux radioélectriques doit se faire en tenant compte des prescriptions liées à la protection du public par rapport aux champs électromagnétiques et notamment aux rayons non-ionisants.

Tout exploitant de réseau de communications électroniques, d'équipements, d'installations et de réseaux radioélectriques est tenu de s'y conformer et veille à ce que les valeurs limites d'exposition des personnes aux champs électromagnétiques définies par décret pris en Conseil des ministres soient respectées dès lors que le public y est exposé.

L'Autorité de régulation s'assure du respect des dispositions de cet article.

Chapitre 3 : Numérotation, noms de domaine

Article 276 Établissement et gestion du plan national de numérotation téléphonique

Le plan national de numérotation téléphonique garantit un accès égal et simple des utilisateurs aux différents réseaux et services de communications électroniques ainsi qu'aux numéros d'urgence, à l'annuaire et aux renseignements publics et l'équivalence des formats de numérotation.

L'établissement et la gestion du plan national de numérotation téléphonique et l'assignation des ressources nationales de numérotation sont assurés par l'Autorité de régulation.

Article 277 Modalités d'attribution des préfixes, numéros et blocs de numéros

L'Autorité de régulation octroie aux opérateurs qui le demandent, dans des conditions qu'elle détermine qui doivent être objectives, transparentes et non discriminatoires, des droits d'utilisation de ressources de numérotation, en tenant compte des impératifs liés à une gestion optimale du plan de numérotation téléphonique. L'Autorité de régulation ne limite pas les ressources de numérotation à attribuer, sauf si cela s'avère nécessaire pour garantir l'utilisation efficace des ressources de numérotation.

La décision d'attribution précise les conditions d'utilisation de ces ressources de numérotation, qui portent sur :

- le type de service auquel l'utilisation des ressources de numérotation attribuées est réservée ;

- les prescriptions nécessaires pour assurer une bonne utilisation des ressources de numérotation attribuées ;

- le cas échéant, les prescriptions relatives à la portabilité du numéro ;

- la durée de l'attribution.

L'Autorité de régulation octroie aux opérateurs les droits d'utilisation des codes utilisés pour l'acheminement des communications électroniques qui ne relèvent pas du système de l'adressage de l'Internet dans les mêmes conditions.

Article 278 Frais et redevances

L'octroi de droits d'utilisation de ressources de numérotation à un opérateur donne lieu au paiement d'une redevance d'utilisation. Les modalités de versement et le montant de ces redevances sont précisés par décret.

Ces redevances sont recouvrées comme les créances de l'Etat relatives au domaine.

L'octroi de droits d'utilisation de ressources de numérotation fait l'objet de frais de gestion fixés par voie règlementaire.

Article 279 Incessibilité des ressources de numérotation et absence de protection par des droits de propriété intellectuelle

L'Autorité de régulation veille à la bonne utilisation des ressources de numérotation et codes attribués.

Ceux-ci ne peuvent être protégés par un droit de propriété industrielle ou intellectuelle et ne peuvent faire l'objet d'un transfert qu'avec l'autorisation préalable de l'Autorité de régulation.

Article 280 Publicité des attributions de numéros

L'Autorité de régulation publie le plan national de numérotation téléphonique sous la seule réserve des restrictions imposées pour des motifs de sécurité nationale.

Article 281 Droits d'utilisation de ressources de numérotation attribués à titre expérimental

L'Autorité de régulation peut octroyer des droits d'utilisation des ressources de numérotation et des codes à titre expérimental en vue d'accompagner le développement d'une technologie ou d'un service innovant du point de vue technique ou commercial.

Ces droits d'utilisation peuvent préciser qu'au titre de l'activité ou du service concerné, et pour une durée maximale de deux ans à compter de leur entrée en vigueur, les droits et obligations du titulaire attachés à la délivrance des droits d'utilisation sont aménagés ou qu'il n'est pas soumis à tout ou partie de ces obligations.

Ils peuvent être assortis d'obligations relatives à l'information des utilisateurs finals concernant le caractère expérimental de l'activité ou du service concerné, ainsi qu'aux modalités de mise en conformité, à l'issue de l'expérimentation, avec les obligations auxquelles il a été dérogé.

Article 282 Gestion du nom de domaine « .dj »

Le Ministère en charge des communications électroniques définit les orientations et les principes de gestion des noms de domaine rattachés à chaque domaine de premier niveau du système d'adressage par domaines de l'internet correspondant aux codes pays du territoire national (« .dj ») dont la mise en œuvre est assurée par l'Autorité de régulation.

L'attribution et la gestion des noms de domaine rattachés à chaque domaine de premier niveau du système d'adressage par domaines de l'internet correspondant aux codes pays du territoire national (« .dj ») sont centralisées par un organisme unique dénommé « registre ».

Le registre attribue et gère les noms de domaine selon les règles fixées par l'Autorité de régulation et lui remet chaque année un rapport d'activité.

Les noms de domaine sont notamment attribués et gérés dans l'intérêt général selon des règles objectives, non discriminatoires et transparentes, garantissant le respect de la liberté de communication, de la liberté d'entreprendre et des droits de propriété intellectuelle. Les noms de domaine sont attribués pour une durée limitée et renouvelable.

L'enregistrement des noms de domaine s'effectue sur la base des déclarations faites par le demandeur et sous sa responsabilité.

Titre 7 Droits de passage sur le domaine public et servitudes

Chapitre premier : Occupation du domaine public et servitudes sur les propriétés privées

Article 283 Principes généraux

Les opérateurs et exploitants d'infrastructures passives bénéficient d'un droit de passage sur le domaine public routier et non routier et de servitudes sur les propriétés privées nécessaires à l'installation, l'exploitation et l'entretien de réseaux de communications électroniques.

Article 284 Droit d'accès aux points hauts

Sans préjudice des dispositions du Titre 4 du présent livre et sous réserve des servitudes radioélectriques instituées et de la disponibilité de l'espace nécessaire, les opérateurs et exploitants d'infrastructures passives bénéficient du droit d'accéder à tous les points hauts existants. L'accès aux points hauts peut faire l'objet d'une rémunération ou d'une indemnisation visant à prendre en charge une part raisonnable des frais d'occupation des lieux. La co-implantation ou le partage des installations en points hauts entre opérateurs est encouragée et fait l'objet de conventions dans les conditions fixées au Titre 4 du présent livre.

Article 285 Conditions générales d'installation des infrastructures, équipements et travaux

L'installation des infrastructures et des équipements doit être réalisée dans le respect de l'environnement et de la qualité esthétique des lieux, et dans les conditions les moins dommageables pour les propriétés privées et le domaine public.

Le domaine public routier et non routier peut être occupé par les opérateurs et exploitants d'infrastructures passives pour y implanter des ouvrages, infrastructures et équipements dans la mesure où cette occupation n'est pas incompatible avec son affectation ou avec les capacités disponibles.

Article 286 Occupation du domaine public non routier

L'occupation du domaine public non routier fait l'objet d'une autorisation d'occupation octroyée par l'autorité concessionnaire ou gestionnaire du domaine.

L'autorisation doit être octroyée dans des conditions transparentes et non discriminatoires. L'autorisation donnant accès au domaine public non routier ne peut contenir de dispositions relatives aux conditions commerciales d'exploitation.

L'occupation du domaine public non routier peut donner lieu au versement d'une redevance à l'autorité concessionnaire ou gestionnaire du domaine dans le respect du principe d'égalité. Cette redevance doit être raisonnable et proportionnée à l'usage du domaine.

Les autorités concessionnaires ou gestionnaires du domaine public non routier se prononcent dans un délai de deux mois suivant la demande présentée par un opérateur ou un exploitant d'infrastructures passives.

Article 287 Occupation du domaine public routier

L'occupation du domaine public routier fait l'objet d'une permission de voirie délivrée par l'autorité compétente suivant la nature de la voie empruntée dans les conditions fixées par la loi.

Les permissions de voirie sont octroyées dans des conditions transparentes et non discriminatoires. La permission de voirie prescrit les conditions d'implantation et d'exploitation nécessaires pour garantir la circulation publique et à la conservation de la voirie. Elle ne peut contenir de dispositions relatives aux conditions commerciales d'exploitation.

L'occupation du domaine public non routier peut donner lieu au versement d'une redevance à l'autorité compétente dans le respect du principe d'égalité. Cette redevance doit être raisonnable et proportionnée à l'usage du domaine.

Les travaux nécessaires à l'établissement et à l'entretien des réseaux et de leurs abords sont effectués conformément aux règlements de voirie.

L'autorité compétente pour délivrer la permission de voirie se prononce dans un délai de deux mois suivant la demande présentée par un opérateur ou un exploitant d'infrastructures passives.

Article 288 Servitudes sur les propriétés privées

Des servitudes sur les propriétés privées sont instituées en vue de permettre l'installation, l'exploitation et l'entretien d'équipements composant les réseaux de communications électroniques ouverts au public et les infrastructures passives, ainsi que pour permettre les opérations d'entretien de leurs abords, notamment le débroussaillage, la coupe d'herbe, l'élagage et l'abattage :

1. sur les bâtiments d'habitation et sur et dans les parties des immeubles collectifs et des lotissements affectées à un usage commun ;

2. sur le sol et dans le sous-sol des propriétés non bâties ;

3. sur et au-dessus des propriétés privées, y compris à l'extérieur des murs ou des façades donnant sur la voie publique, dans la mesure où l'opérateur se borne à utiliser l'installation d'un tiers bénéficiant de servitudes sans compromettre, le cas échéant, la mission propre de service public confiée à ce tiers. En cas de contrainte technique, l'installation est déployée à proximité de celle déjà existante, en suivant au mieux son cheminement.

Les servitudes sur les propriétés privées sont établies sur autorisation délivrée par décision du maire au nom de l'Etat après que les propriétaires, ou, en cas de copropriété, le syndicat des copropriétaires représenté par le syndic, ont été informés des motifs qui justifient l'établissement de la servitude et le choix de son emplacement, et été mis à même, dans un délai qui ne peut pas être inférieur à trois mois, de présenter leurs observations sur le projet de servitude. Les travaux ne peuvent commencer avant l'expiration de ce délai. En cas de contestation, les modalités de mise en œuvre de la servitude sont fixées par le président du Tribunal de première instance.

L'installation d'équipements sur les propriétés privées ne peut faire obstacle au droit des propriétaires ou copropriétaires de démolir, réparer, modifier ou clore leur propriété. Toutefois, les propriétaires ou copropriétaires doivent, au moins trois mois avant d'entreprendre des travaux de nature à affecter les équipements, prévenir le bénéficiaire de la servitude.

Lorsque, pour l'étude, la réalisation, l'exploitation et l'entretien des équipements ou pour les opérations d'entretien du réseau mentionnées au premier alinéa, l'introduction des agents de l'opérateur bénéficiaire de la servitude dans les propriétés privées est

nécessaire, elle est, à défaut d'accord amiable ou de convention conclue entre le propriétaire et l'opérateur, autorisée par le président du Tribunal de première instance statuant en référé qui s'assure que la présence des agents est nécessaire.

Le bénéficiaire de la servitude est responsable de tous les dommages qui trouvent leur origine dans les équipements du réseau. Il est tenu d'indemniser l'ensemble des préjudices directs et certains causés tant par les travaux d'installation et d'entretien que par l'existence ou le fonctionnement des équipements. A défaut d'accord amiable, l'indemnité est fixée par la juridiction de l'expropriation saisie par la partie la plus diligente.

Dès lors qu'elle n'accroît pas l'atteinte portée à la propriété privée, la servitude prévue au 3 du présent article est exemptée de la procédure d'autorisation prévue au cinquième alinéa mais peuvent donner lieu à indemnisation dans les conditions prévues à l'alinéa précédent.

Article 289 Péremption des autorisations d'occupation, permissions de voirie et servitudes

Les autorisations d'occupation du domaine public non routier, les permissions de voirie sur le domaine public routier et les servitudes sur les propriétés privées établies ou octroyées pour l'établissement et l'exploitation de réseaux de communications électroniques ou d'infrastructures passives expirent de plein droit s'il n'est suivi d'un commencement d'exécution des travaux dans les six mois de leur entrée en vigueur.

Article 290 Mutualisation des droits de passage et des servitudes sous l'égide de l'Autorité de régulation

Lorsqu'il est constaté que le droit de passage sur le domaine public routier ou la servitude de l'opérateur ou de l'exploitant d'infrastructures passives peut être assuré, dans des conditions équivalentes à celles qui résulteraient d'une occupation du domaine public autorisée ou du bénéfice de cette servitude, par l'utilisation des installations existantes d'un autre occupant du domaine public routier ou d'un autre bénéficiaire de servitude ou d'une convention de passage signée avec le propriétaire sur la propriété concernée et que cette utilisation ne compromettrait pas la mission propre de service public de cet occupant ou du bénéficiaire de la servitude ou de la convention de passage, l'autorité compétente peut inviter les deux parties à se rapprocher pour convenir des conditions techniques et financières d'une utilisation partagée des équipements et installations en cause.

Dans ce cas, et sauf accord contraire, le propriétaire des installations accueillant l'opérateur ou l'exploitant d'infrastructures passives autorisé assume, dans la limite du contrat conclu entre les parties, l'entretien des infrastructures et des équipements, et s'agissant du domaine public non routier, y compris de leurs abords, qui empruntent ses

installations et qui sont placés sous sa responsabilité, moyennant paiement d'une contribution négociée avec l'opérateur.

Article 291 Charge de la réalisation des travaux d'entretien des abords des réseaux de communications électroniques

Les opérations d'entretien des abords d'un réseau de communications électroniques ouvert au public oud'infrastructures passives telles que le débroussaillage, la coupe d'herbe, l'élagage et l'abattage sont accomplies par le propriétaire du terrain, le fermier ou leurs représentants, que le réseau soit implanté sur la propriété ou non et, que la propriété soit riveraine ou non du domaine public, afin de permettre le déploiement de réseaux et de prévenir l'endommagement des équipements du réseau et l'interruption du service. A cette fin, l'opérateur concerné est tenu de proposer au propriétaire du terrain, au fermier ou à leurs représentants l'établissement d'une convention.

En cas de défaillance de leur part, ces opérations sont accomplies par l'opérateur ou l'exploitant d'infrastructures passives aux frais du propriétaire du terrain, du fermier ou de leurs représentants. L'exécution des travaux doit être précédée d'une notification qui leur est adressée ainsi qu'au maire de la commune sur le territoire de laquelle la propriété est située. L'introduction des agents de l'opérateur ou de l'exploitant d'infrastructures passives en vue de procéder aux opérations d'entretien s'effectue selon les modalités prévues à l'Article 288.

Par dérogation aux deux alinéas précédents, les opérations d'entretien sont accomplies par l'opérateur ou l'exploitant d'infrastructures passives lorsque :

- le propriétaire du terrain, le fermier ou leurs représentants ne sont pas identifiés ;

- l'opérateur ou l'exploitant d'infrastructures passives et le propriétaire du terrain, le fermier ou leurs représentants en sont convenus ainsi par convention, notamment lorsque les coûts exposés par ces opérations sont particulièrement élevés pour ces derniers ou lorsque la réalisation de ces opérations présente des difficultés techniques ou pratiques de nature à porter atteinte à la sécurité ou à l'intégrité des réseaux.

Sur le domaine public, les modalités de réalisation de ces opérations d'entretien sont définies par l'autorisation d'occupation ou la permission de voirie le cas échéant.

Chapitre 2 : Servitudes radioélectriques

Article 292 Consultation préalable de l'Autorité de régulation et tenue d'un registre des servitudes radioélectriques

L'Autorité de régulation est consultée sur tous les projets de servitudes radioélectriques instituées dans les conditions prévues dans le présent livre. Elle constitue, tient à jour et publie la documentation relative aux servitudes établies dans ce domaine au titre des différents ministères.

En liaison avec les services et organismes compétents, elle établit et publie les documents, les répertoires et les fichiers relatifs aux installations radioélectriques et aux zones de groupement des installations radioélectriques.

Article 293 Institution des servitudes radioélectriques contre les obstacles ou les perturbations électromagnétiques

Afin d'assurer la propagation des ondes radioélectriques émises ou reçues par les centres radioélectriques exploités ou contrôlés par les services de l'Etat, l'autorité administrative compétente peut instituer des servitudes radioélectriques d'utilité publique pour la protection des communications électroniques par voie radioélectrique contre les obstacles ou des réceptions radioélectriques contre les perturbations électromagnétiques.

Ces servitudes obligent les propriétaires, les titulaires de droits réels ou les occupants concernés à s'abstenir de tout fait de nature à nuire au bon fonctionnement de ces centres radioélectriques.

Dans le cas où, dans le cadre de la procédure d'instruction d'une servitude radioélectrique, il est nécessaire d'accéder aux propriétés privées pour la réalisation de mesures de compatibilité électromagnétique, les propriétaires, titulaires de droits réels ou occupants sont tenus de laisser libre cet accès. A défaut d'accord des propriétaires, titulaires de droits réels ou occupants, il y est procédé dans les conditions fixées par la loi.

Les servitudes radioélectriques sont instituées après information des propriétaires, titulaires de droits réels ou occupants dans le cadre d'une enquête publique. Lorsque les conclusions de l'enquête publique sont défavorables à l'instauration de la servitude, celle-ci est instaurée par décret.

Article 294 Indemnisation

L'institution des servitudes radioélectriques ouvre droit à indemnisation s'il en résulte une modification de l'état antérieur des lieux entraînant un dommage direct, matériel et certain.

Le montant de l'indemnisation, à défaut de règlement amiable, est fixé par le Tribunal Administratif de Première Instance.

Sous peine de forclusion, la demande d'indemnisation doit parvenir au service de l'Etat qui exploite ou contrôle le centre radioélectrique au profit duquel a été instituée la servitude radioélectrique dans un délai d'un an à compter de la date de notification aux intéressés des sujétions dont ils font l'objet.

Article 295 Expropriation des immeubles pour utilité publique

Lorsque les servitudes radioélectriques entraînent la suppression ou la modification de bâtiments constituant des immeubles par nature en application des articles 658 et suivants du code civil, il est procédé, à défaut d'accord amiable, à expropriation pour cause d'utilité publique dans les conditions fixées par la loi.

Après suppression ou modification des bâtiments ainsi acquis et lorsque les lieux ont été mis en conformité avec les exigences du présent chapitre, il peut être procédé à la revente des immeubles expropriés, sous garantie d'un droit de préemption aux propriétaires dépossédés et sous réserve du respect par l'acquéreur de ces servitudes.

Article 296 Obligation de se conformer aux servitudes contre les perturbations électromagnétiques et indemnisation

Tout propriétaire ou toute personne faisant l'usage d'une installation électrique, même située hors des zones de servitudes radioélectriques, produisant ou propageant des perturbations électromagnétiques gênant l'exploitation d'un centre de réception radioélectrique exploité ou contrôlé par les services de l'Etat protégé par une servitude radioélectrique, est tenu de se conformer aux dispositions qui lui sont prescrites en vue de faire cesser le trouble par l'autorité administrative compétente dont les services exploitent ou contrôle le centre radioélectrique, et se prête notamment aux investigations demandées et réalise les modifications indiquées afin de maintenir les installations en bon état de fonctionnement.

Lorsque le propriétaire ou la personne faisant l'usage de l'installation électrique ne procède pas aux modifications prescrites, il y est procédé d'office à ses frais et risques.

Lorsque l'exécution des obligations prescrites au premier alinéa cause un dommage direct, matériel et certain au propriétaire ou à la personne faisant l'usage de l'installation radioélectrique, il est fait application des dispositions de l'Article 294 .

Chapitre 3 : Servitudes de protection des câbles et lignes de réseaux de communications électroniques en raison d'obstacles ou d'exécution de travaux

Article 297 Institution des servitudes de protection

Des servitudes de protection des câbles et des lignes de réseaux de communications électroniques peuvent être instituées afin d'assurer la conservation et le fonctionnement normal desdits réseaux.

Article 298 Indemnisation

L'institution de ces servitudes ouvre droit à indemnisation s'il en résulte un dommage direct, matériel et actuel.

Le montant de l'indemnisation, à défaut de règlement amiable, est fixé par la juridiction compétente.

Sous peine de forclusion, la demande d'indemnisation doit parvenir au bénéficiaire des servitudes dans un délai d'un an à compter de la date de notification aux intéressés des sujétions dont ils font l'objet.

Titre 8 Service universel

Chapitre premier : Principes généraux

Article 299 Stratégie de déploiement du service universel

La stratégie de déploiement du service universel des communications électroniques s'inscrit dans le cadre d'une concertation et d'efforts multisectoriels pour tirer parti des synergies des déploiements des réseaux sur le territoire de la République de Djibouti.

A cet effet, l'Autorité de régulation évalue et identifie périodiquement les besoins de la population sur le territoire national d'accès aux différentes composantes du service universel des communications électroniques et recommande Ministre chargé des communications électroniques une stratégie de déploiement identifiant des zones à desservir et des projets spécifiques à mettre en œuvre en priorité sur une période de trois (3) ans. Le gouvernement adopte par décret pris en Conseil des ministres la stratégie de déploiement du service universel des communications électroniques proposée par le Ministre chargé des communications électroniques après concertation avec les Ministères chargés de l'énergie, de la distribution d'eau potable et de l'aménagement du territoire.

Le Ministère chargé des communications électroniques, sur la recommandation de l'Autorité de régulation, actualise la stratégie de déploiement du service universel en

prenant en compte, entre autres, les évolutions sociales, économiques et technologiques et l'évolution des besoins et formule une nouvelle proposition de stratégie tous les trois (3) ans.

Les modalités d'application du présent article sont fixées par décret pris en Conseil des ministres.

Article 300 Promotion des services innovants et des prix abordables

Afin de faciliter l'accès aux services de communications électroniques, le Ministère en charge des communications électroniquespromeut, avec l'appui de l'Autorité de régulation :

- l'introduction de services innovants mettant en œuvre de nouvelles technologies qui offrent des options variées à des prix abordables dans un cadre transparent et non discriminatoire ;

- la fourniture d'équipements terminaux à des prix abordables ;

- l'installation de points d'accès publics gratuits ou payants aux services compris dans le service universel dans des centres d'intérêts communautaires.

Article 301 Objectifs du service universel, composantes et services inclus

Le service universel des communications électroniques vise à fournir à tous, sur l'ensemble du territoire national :

- un raccordement ou un accès à un réseau de communications électroniques ouvert au public fixe ou mobile, un service téléphonique et un service d'accès à Internet de qualité, avec un débit suffisant et à un prix abordable et permettant l'acheminement gratuit des appels d'urgence ;

- un service de renseignements et un annuaire d'utilisateurs, sous formes imprimée ou électronique ;

- des points d'accès aux services de communications électroniques gratuits ou payants accessibles à tout utilisateur, dans des conditions raisonnables en termes de nombre et de répartition géographique ;

- des mesures particulières en faveur des utilisateurs finals ayant des besoins spécifiques afin de leur assurer un accès aux services précités équivalent à l'accès dont bénéficient les autres utilisateurs finals et à un coût abordable.

Le service universel est fourni dans des conditions tarifaires et techniques prenant en compte les difficultés particulières rencontrées dans l'accès au service téléphonique par

certaines catégories de personnes, en raison notamment de leur niveau de revenu et en proscrivant toute discrimination fondée sur la localisation géographique de l'utilisateur.

L'Autorité de régulation peut, en tant que de besoin, préciser les caractéristiques et le contenu de chacune des composantes du service universel et en ajouter de nouvelles.

Chapitre 2 : Mise en œuvre du service universel

Article 302 Financement du service universel par un fonds spécial

Il est créé un fonds destiné au financement du service universel, appelé « Fonds du Service Universel », dont la gestion comptable et financière est assurée par l'Autorité de régulation.

Les modalités de fonctionnement et de gestion dudit fonds peuvent être précisées par décret pris en Conseil des ministres.

Article 303 Ressources du Fonds du Service Universel

Les ressources du Fonds du Service Universel sont :

1. Les contributions au service universel, conformément à l'Article 308 ;
2. Les dons et legs ;
3. Les subventions de partenaires au développement ;
4. Toute autre contribution décidée par l'Autorité de régulation.

Les ressources du Fonds du Service Universel sont consacrées aux activités visant à la réalisation des missions assignées au service universel des communications électroniques, conformément aux dispositions du présent Titre.

Un compte spécial destiné aux ressources du Fonds du Service Universel, distinct des autres comptes de l'Autorité de régulation, est créé par ladite Autorité de régulation. Les opérations de ce compte sont budgétisées et comptabilisées séparément des autres opérations de l'Autorité de régulation.

Le compte spécial du Fonds du Service Universel est géré par l'Autorité de régulation.

Article 304 Comité de gestion du Fonds du Service Universel

Sur la base de la stratégie définie par l'Autorité de régulation, le Comité de gestion du Fonds de Service Universel :

- Propose les programmes de réalisation du service universel ;

- Précise pour chaque programme le contenu et les coûts prévisionnels de réalisation ;
- Désigne les exploitants et prestataires chargés de la réalisation desdits programmes ;
- Approuve les marchés pour la réalisation desdits programmes.

Article 305 Composition du Comité de gestion du Fonds de Service Universel

Le Comité de gestion du Fonds de Service Universel est un organe collégial délibérant composé comme suit :

- Lereprésentant de la Présidence de la République ;
- Le représentant du Ministère en charge de l'Economie et des Finances ;
- Le représentant du Ministère en charge du budget ;
- Le représentant du Ministère en charge des communications électroniques ;
- Le représentant du Ministèreen chargede l'économie numérique ;
- les représentants des opérateurs titulaires d'une licence de téléphonie fixe ou mobile ;
- Du représentant des fournisseurs d'accès internet ;
- Du directeur général de l'Autorité de régulation, qui assure le secrétariat.

A l'exception du Directeur Général de l'Autorité de Régulation Multisectorielle de Djibouti, les membres du Comité de gestion du Fonds de Service Universel sont nommés par décret présidentiel, pour un mandat de trois (3) ans, renouvelable une seule fois.

Ils peuvent être révoqués dans les mêmes formes.

Lorsqu'un membre du Comité de gestion démissionne ou décède au cours de l'exercice de ses fonctions, il est immédiatement pourvu à son remplacement dans les mêmes conditions et forme.

Les fonctions de membre donnent droit à des indemnités fixées conjointement par la présidence de la république et le ministère en charge du budget.

Le Comité de gestion adopte son règlement intérieur, qui est approuvé par la présidence de la république

Article 306 Modalités de sélection des opérateurs chargés du service universel

En vue de garantir la fourniture du service universel sur l'ensemble du territoire national conformément à la stratégie de déploiement du service universel, l'Autorité de régulation peut sélectionner, pour les composantes ou éléments des composantes du service universel à fournir identifiés dans la stratégie, un ou plusieurs opérateurs chargés de fournir cette composante ou cet élément.

La sélection intervient à l'issue d'appels à candidatures sur la base d'un projet de cahier des charges établi par l'Autorité de régulation portant notamment sur les conditions techniques et financières de fourniture de cette composante ou élément, y compris les objectifs de desserte de zones du territoire national, de performance, de qualité de service, les conditions tarifaires de fourniture du service, ainsi que le coût net de fourniture du service universel envisagé. La sélection peut prendre en compte le montant de compensation demandé par les candidats dans l'objectif de réduire le montant de financement nécessaire par le fonds de service universel ainsi que des mécanismes visant à atteindre un équilibre financier, notamment par l'utilisation de technologies peu coûteuses et innovantes.

Dans le cas où un appel à candidatures s'avère infructueux, l'Autorité de régulation peut désigner d'office un ou plusieurs opérateurs en vue d'assurer la composante du service en cause dans les conditions fixées par elle.

L'Autorité de régulation veille à la mise en œuvre des programmes de service universel et au respect par les opérateurs désignés des obligations mises à leur charge.

Un décret pris en Conseil des ministres détermine les modalités d'application du présent article. Il fixe notamment les conditions dans lesquelles les opérateurs sont sélectionnés et les tarifs du service universel et sa qualité sont contrôlés.

Article 307 Compensation des coûts du service universel

Les recettes et les dépenses imputables aux composantes du service universel assurées par un opérateur sont retracées au sein d'une comptabilité distincte. Sur la base de cette comptabilité distincte, les coûts nets des obligations de fourniture du service universel sont évalués par l'Autorité de régulation, et comprennent :

- les coûts nets des obligations tarifaires correspondant aux obligations de péréquation géographique des tarifs de la composante du service universel assurée par l'opérateur ;

- les coûts nets de l'offre et des obligations correspondant à la composante du service universel assurée par l'opérateur ; et

- la rémunération du capital utilisé au titre du service universel, prenant en compte l'avantage sur le marché que l'opérateur retire, le cas échéant, de ses obligations de service universel.

Le coût net de fourniture du service universel est rendu public par l'Autorité de régulation.

Lorsque l'Autorité de régulation détermine que la fourniture du service universel représente une charge injustifiée pour l'opérateur désigné comme fournisseur, au vu du coût net de fourniture du service universel évalué par elle, l'Autorité de régulation fixe le montant de la compensation qui peut être accordée à l'opérateur.

La comptabilité tenue par les opérateurs désignés pour assurer la fourniture d'une ou plusieurs composantes du service universel est auditée, à leurs frais, par un organisme désigné par l'Autorité de régulation.

Ne peuvent faire l'objet d'une compensation le coût de mise en œuvre des obligations d'acheminer gratuitement les appels d'urgence et de prendre des mesures particulières en faveur des utilisateurs finals ayant des besoins spécifiques dans la mesure où elles s'imposent à tout opérateur dans sa zone de desserte.

Un décret pris en Conseil des ministres précise les méthodes de l'évaluation qui répondent à des exigences de transparence et de publicité, de la compensation et du partage des coûts nets du service universel.

Article 308 Contribution des opérateurs au service universel des communications électroniques

Les opérateurs sont tenus de contribuer au service universel des communications électroniques soit en réalisant des investissements pour mettre en œuvre des programmes de service universel initiés par l'Autorité de régulation conformément à la stratégie de déploiement du service universel conformément à l'Article 306 soit en contribuant annuellement au fonds destiné au financement du service universel.

Le montant de la contribution au fonds due par les opérateurs est calculé par un pourcentage du chiffre d'affaires hors taxes net des frais d'interconnexion réglés entre les opérateurs. Ledit pourcentage est fixé par voie réglementaire. Le montant des investissements réalisés par les opérateurs qui mettent en œuvre des programmes de service universel est déduit de la contribution qu'ils sont tenus de verser au fonds.

Les contributions des opérateurs sont collectées par l'Autorité de régulation.

Les opérateurs dont le chiffre d'affaires est inférieur à un montant fixé par le décret prévu ci-dessus sont exonérés de contribution au fonds de service universel.

Titre 9 Contrôle, règlement des différends et sanctions

Chapitre premier : Contrôle et suivi des opérateurs

Section 1 : Dispositions modificatives

Article 309 Droit de communication

Les personnes exerçant des activités dans les secteurs régulés sont tenues de fournir à l'Autorité de régulation annuellement, et à tout moment sur demande, les informations ou documents, y compris les informations financières, qui lui permettent de s'assurer du respect de la législation et de la réglementation applicables ainsi que des obligations spécifiquement mises à leur charge au titre du régime juridique dont relève leur activité au regard de la réglementation sectorielle.

Les personnes concernées fournissent ces informations en respectant les délais et le niveau de détail exigés par l'Autorité de régulation.

Les informations demandées par l'Autorité de régulation doivent être proportionnées aux besoins nécessaires à l'accomplissement de ses missions. L'Autorité de régulation indique les motifs justifiant ses demandes d'informations.

Le secret des affaires n'est pas opposable à l'Autorité de régulation ; toutefois celle-ci est tenue de respecter la confidentialité des informations reçues.

Section 2 : Dispositions spécifiques au secteur des communications électroniques

Article 310 Compétence de l'Autorité de régulation

Conformément aux dispositions des articles 5 et 6 de la loi n° 74/AN/20/8ème L du 13 février 2020 portant création de l'Autorité de régulation multisectorielle de Djibouti, l'Autorité de régulation veille au respect des dispositions du présent titre et des textes et décisions pris pour leur application et contrôle le respect par les opérateurs et toute personne qui y est soumise des obligations qui leur incombent. Sans préjudice des dispositions de l'article 7 de ladite loi, l'Autorité de régulation peut mener des enquêtes, procéder à des contrôles et visites et obtenir communication de tout document nécessaire à l'exercice de ses missions conformément aux dispositions du présent chapitre.

Article 311 Habilitation des fonctionnaires et agents de l'Autorité de régulation

L'Autorité de régulation peut, par décision particulière, charger un ou plusieurs fonctionnaires et agents de ses services de procéder à des contrôles et des vérifications portant sur toute activité soumise aux dispositions du présent livre.

Ceux des fonctionnaires et agents de l'Autorité de régulation qui peuvent être appelés à participer à la mise en œuvre de ses missions de contrôle en application du présent chapitre doivent y être habilités par l'Autorité de régulation. Cette habilitation ne dispense pas de l'application des dispositions définissant les procédures autorisant l'accès aux secrets protégés par la loi et assurant la protection des libertés individuelles.

Article 312 Pouvoir d'enquête et droit de visite

Les fonctionnaires et agents assermentés de l'Autorité de régulation habilités à cet effet ont accès, dans les conditions prévues par le code de procédure pénale, pour l'exercice de leurs missions, aux lieux, locaux, enceintes, installations ou établissements utilisés par des personnes se livrant à des activités soumises aux dispositions du présent livre et qui sont à usage professionnel, à l'exclusion des parties de ceux-ci affectées à un usage d'habitation.

Le procureur de la République en est préalablement informé.

En cas d'opposition du responsable des lieux, ou lorsqu'il s'agit de lieux mentionnés au premier alinéa affectés à un usage d'habitation, la visite ne peut se dérouler qu'avec l'autorisation du président du Tribunal de première instance ou du juge délégué par lui. Toutefois, lorsque l'urgence, la gravité des faits à l'origine du contrôle ou le risque de destruction ou de dissimulation de documents le justifie, la visite peut avoir lieu sans que le responsable des locaux en ait été informé, sur autorisation préalable du président du Tribunal de première instance. Dans ce cas, le responsable des lieux ne peut s'opposer à la visite. La visite s'effectue sous l'autorité et le contrôle du président du Tribunal de première instance ou du juge délégué par lui, en présence de l'occupant des lieux ou de son représentant qui peut se faire assister d'un conseil de son choix ou, à défaut, en présence de deux témoins qui ne sont pas placés sous l'autorité des personnes chargées de procéder au contrôle.

Le président du Tribunal de première instance est saisi à la requête du président de l'Autorité de régulation. Il statue par ordonnance motivée dans les conditions prévues par la loi. L'ordonnance est exécutoire au seul vu de la minute. Elle mentionne que le juge ayant autorisé la visite peut être saisi à tout moment d'une demande de suspension ou d'arrêt de cette visite et indique les voies et délais de recours.

Article 313 Recueil de documents, saisies

Sans préjudice des dispositions de l'article 9 de la loi n° 74/AN/20/8ème L du 13 février 2020 portant création de l'Autorité de régulation multisectorielle de Djibouti, les fonctionnaires et agents assermentés de l'Autorité de régulation habilités à cet effet 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. Ils peuvent accéder aux programmes informatiques et aux données stockées et en demander la transcription par tout traitement approprié dans des documents directement utilisables pour les besoins du contrôle. Ils peuvent être assistés par des experts choisis par l'Autorité de régulation.

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

Pour le contrôle de services de communication au public en ligne, les fonctionnaires et agents assermentés de l'Autorité de régulation habilités à cet effet peuvent réaliser toute opération en ligne nécessaire à leur mission sous une identité d'emprunt. À peine de nullité, leurs actes ne peuvent constituer une incitation à commettre une infraction. L'utilisation d'une identité d'emprunt est sans incidence sur la régularité des constatations effectuées.

Les fonctionnaires et agents assermentés de l'Autorité de régulation habilités à cet effet peuvent, avec l'autorisation et sous le contrôle du président du Tribunal de première instance ou du juge délégué par lui saisi dans les conditions fixées par l'Article 312 , procéder au contrôle des équipements et à la saisie des matériels. La demande de l'autorisation précitée doit comporter tous les éléments d'information de nature à justifier la saisie. Les matériels saisis sont immédiatement inventoriés. A titre de mesure conservatoire, les fonctionnaires et agents assermentés de l'Autorité de régulation habilités à cet effet peuvent procéder à la mise sous scellés des matériels et équipements dès la constatation de l'infraction.

Article 314 Établissement de procès-verbaux

Il est dressé contradictoirement procès-verbal des contrôles, vérifications, visites et saisies effectuées par les fonctionnaires et agents habilités de l'Autorité de régulation conformément aux dispositions du présent chapitre.

Leurs procès-verbaux sont transmis dans les cinq jours aux personnes intéressées et, le cas échéant, au président du Tribunal de première instance ou au juge délégué par lui qui a autorisé la visite et/ou la saisie. Ils font foi jusqu'à preuve contraire.

Chapitre 2 : Règlement des différends

Article 315 Modalités de saisine de l'Autorité de régulation

Conformément à l'article 7 de la loi n° 74/AN/20/8ème L du 13 février 2020 portant création de l'Autorité de régulation multisectorielle de Djibouti, l'Autorité de régulation peut être saisie par l'une quelconque des parties en vue de faciliter le règlement des différends portant sur :

- l'interconnexion et l'accès aux réseaux de communications électroniques ouverts au public et aux autres formes particulières d'accès, y compris l'accès aux infrastructures passives et aux infrastructures alternatives, notamment en cas de refus, d'échec des négociations commerciales ou de désaccord sur la conclusion ou l'exécution d'une convention ; et

- l'utilisation partagée entre opérateurs d'installations existantes situées sur le domaine public routier ou sur une propriété privée conformément à l'Article 290, en cas d'échec des négociations.

L'Autorité de régulation peut également être saisie par un utilisateur, y compris par l'intermédiaire d'une association de défense des intérêts des consommateurs ou une association professionnelle, en cas de différend avec un opérateur n'ayant pu être résolu à travers le mécanisme de traitement des réclamations mis en place par l'opérateur conformément à l'Article 510 portant sur :

- la violation par l'opérateur de dispositions légales ou réglementaires en lien avec la fourniture de services de communications électroniques dont bénéficie l'utilisateur ; et

- la violation par l'opérateur du contrat conclu entre l'utilisateur et l'opérateur ou le caractère abusif de clauses contenues dans ce contrat.

A cet effet, l'Autorité de régulation désigne parmi son personnel une ou plusieurs personnes chargées de recueillir les plaintes des utilisateurs en vue de l'ouverture d'une procédure de règlement de différend.

Article 316 Procédure de règlement des différends

L'Autorité de régulation définit les règles de procédure transparentes et non-discriminatoires selon lesquelles elle tranche les différends qui lui sont soumis. Ces règles prévoient notamment :

- les modalités de saisine de l'Autorité de régulation ;

- les délais et modalités selon lesquels l'Autorité de régulation instruit les demandes et réclamations qui lui sont soumises et rend ses décisions ;

- les modalités de respect du principe du contradictoire et des droits de la défense permettant en particulier aux parties de présenter leurs observations ;

- les modalités de respect de la confidentialité des informations échangées dans le cadre de la procédure qui relèvent du secret des affaires ou de la vie privée des personnes intéressées

- les mesures que peut prononcer l'Autorité de régulation dans le cadre de l'instruction et de la résolution des différends, s'agissant de la communication d'informations à une partie ou à l'Autorité de régulation, de la conformité aux dispositions légales et réglementaires applicables, de la mise en œuvre de mesures correctives ou, en cas d'urgence, de mesures conservatoires, de la modification des conventions ou contrats en cause, de la réparation de préjudices subis ;

- une obligation de motivation, de notification et de publication des décisions de l'Autorité de régulation.

Les parties peuvent se faire assister ou représenter dans le cadre des procédures de règlement de différends.

L'Autorité de régulation peut procéder à des consultations techniques, économiques ou juridiques, ou expertises externes aux fins de trancher le différend. Les frais engendrés par ces consultations et expertises peuvent être mis à la charge de la partie perdante, sauf si les circonstances particulières du différend justifient qu'ils soient mis à la charge d'une autre partie ou partagés entre les parties.

Lorsque, le cas échéant, l'activité de l'exploitant d'infrastructures alternatives concerné relève de la compétence d'une autre Autorité de régulation sectorielle, l'Autorité de régulation saisit celle-ci pour avis avant de se prononcer sur le différend.

Article 317 Recours contre les décisions de règlement de différend

Par dérogation aux dispositions de la loi n° 74/AN/20/8ème L du 13 février 2020 portant création de l'Autorité de régulation multisectorielle de Djibouti, les décisions prises par l'Autorité de régulation en matière de règlement de différend peuvent faire l'objet d'un recours en annulation ou en réformation devant le Tribunal administratif de première instance dans un délai d'un (1) mois à compter de leur notification. Ce délai est de dix (10) jours pour les mesures conservatoires. Dans ce cas, le recours est jugé dans un délai d'un mois.

Le recours n'est pas suspensif. Un sursis à exécution peut être ordonné par le président du Tribunal administratif de première instance saisit sur requête si la décision en cause est susceptible d'entraîner des conséquences manifestement excessives ou s'il est survenu, postérieurement à sa notification, des faits nouveaux d'une exceptionnelle gravité.

Chapitre 3 : Sanctions administratives

Section 1 : Dispositions modificatives et préliminaires

Article 318 Saisine de l'Autorité de régulation

L'Autorité de régulation Multisectorielle de Djibouti peut, soit d'office, soit à la demande d'un Ministère concerné, d'une organisation professionnelle, d'une association d'utilisateurs ou d'une personne physique ou morale concernée, sanctionner les manquements qu'elle constate aux dispositions législatives et réglementaires régissant les secteurs qu'elle régule.

L'Autorité de régulation ne peut être saisie de faits remontant à plus de trois ans, s'il n'a été fait auparavant aucun acte tendant à leur recherche, leur constatation ou leur sanction.

Les modalités d'application des sanctions sont définies par les lois sectorielles et leurs textes d'application.

Article 319 Règles générales de procédure

Lorsqu'elle examine les manquements aux dispositions du présent livre dont elle est saisie ou se saisit d'office et envisage de prononcer des sanctions, l'Autorité de régulation applique les règles de procédure générales fixées par le chapitre VII de la loi n° 74/AN/20/8ème L du 13 février 2020 portant création de l'Autorité de régulation multisectorielle de Djibouti, sous réserve des règles spécifiques au secteur des communications électroniques fixées par la Section 2 du présent chapitre.

Lorsque, le cas échéant, l'activité de l'exploitant d'infrastructures alternatives concerné relève de la compétence d'une autre Autorité de régulation sectorielle, l'Autorité de régulation saisit celle-ci pour avis avant de se prononcer sur les manquements et avant toute décision.

Section 2 : Règles spécifiques applicables aux sanctions administratives prononcées dans le secteur des communications électroniques

Article 320 Mise en demeure préalable

Conformément à l'article 34 de la loi n° 74/AN/20/8ème L du 13 février 2020 portant création de l'Autorité de régulation multisectorielle de Djibouti, en cas de manquement par un opérateur, un exploitant d'infrastructures passives, un exploitant d'infrastructures alternatives, un exploitant de réseau indépendant ou de réseau interne ou un titulaire d'agrément aux dispositions légales et réglementaires au respect desquelles l'Autorité de régulation a pour mission de veiller ainsi qu'aux textes et décisions pris en application de ces dispositions, l'Autorité de régulation le met en demeure de s'y conformer dans un délai qu'elle détermine.

La mise en demeure est motivée et notifiée à l'intéressé. Elle peut être rendue publique par l'Autorité de régulation.

Article 321 Sanctions pouvant être prononcées en cas de non-respect de la mise en demeure

Conformément aux articles 7 et 35 de la loi n° 74/AN/20/8ème L du 13 février 2020 portant création de l'Autorité de régulation multisectorielle de Djibouti, lorsque l'intéressé ne se conforme pas dans les délais fixés à la mise en demeure adressée par l'Autorité de régulation, celle-ci peut adresser une notification de griefs à la personne en cause en vue d'une sanction.

Après que l'intéressé a reçu la notification des griefs et a été mise à même de consulter le dossier et de présenter ses observations écrites, l'Autorité de régulation, avant de prononcer une sanction, procède, selon une procédure contradictoire, à l'audition du rapporteur instructeur du dossier et de l'intéressé qui peut présenter des observations orales. L'Autorité de régulation peut également entendre toute personne dont l'audition lui paraît utile.

L'Autorité de régulation peut prononcer à l'encontre de l'intéressé une sanction pécuniaire :

- si l'intéressé est titulaire d'une licence ou d'une autorisation, d'un montant maximum de quatre pour cent du chiffre d'affaires consolidé du dernier 'exercice comptable ;

- si l'intéressé a souscrit une déclaration ou est titulaire d'un agrément sans détenir de licence ou d'autorisation, ou si ses activités relèvent du régime libre, d'un montant maximum de 1.300.000 DJF à 25.000.000 DJF ;

- si l'intéressé est un exploitant d'infrastructures alternatives, d'un montant maximum de 1.300.000 DJF à 25.000.000 DJF ;

- si l'intéressé est une personne physique, d'un montant maximum de 1.300.000 DJF;

En cas de récidive, le montant maximum de la sanction pécuniaire est doublé.

Le montant de la sanction pécuniaire est fixé en fonction de la gravité des manquements commis et en relation avec les avantages ou les profits tirés de ces manquements.

Si la violation constatée et notifiée persiste, l'Autorité de régulation, peut prononcer, suivant la procédure prévue par le présent chapitre :

- la suspension totale ou partielle de l'autorisation pour une durée de trente jours au plus ;

- la suspension temporaire de l'autorisation ou la réduction de la durée de cette dernière dans la limite d'une année ; ou

- le retrait définitif de l'autorisation.

Elle peut, dans les mêmes conditions, prononcer le retrait définitif de l'agrément ou des droits d'utilisation de fréquences radioélectriques ou de ressources de numérotation ou mettre fin aux effets de la déclaration.

Si l'intéressé est titulaire d'une licence, l'Autorité de régulation peut proposer au ministre chargé des communications électronique que soit décidé par décret pris en Conseil des ministres :

- la suspension totale ou partielle de la licence pour une durée de trente jours au plus ;

- la suspension temporaire de la licence ou la réduction de la durée de cette dernière dans la limite d'une année ; ou

- le retrait définitif de la licence.

Conformément à l'article 36 de la loi n° 74/AN/20/8ème L du 13 février 2020 portant création de l'Autorité de régulation multisectorielle de Djibouti, les décisions de l'Autorité de régulation sont motivées et notifiées à l'intéressé et publiées au Journal officiel.

Article 322 Mesures conservatoires en cas d'urgence

Conformément à l'article 35 de la loi n° 74/AN/20/8ème L du 13 février 2020 portant création de l'Autorité de régulation multisectorielle de Djibouti, en cas d'atteinte grave et immédiate aux dispositions légales et réglementaires au respect desquelles l'Autorité de régulation a pour mission de veiller ainsi qu'aux textes et décisions pris en application de ces dispositions, l'Autorité de régulation peut ordonner, sans mise en demeure préalable, des mesures conservatoires dont la validité est de trois mois au maximum.

Ces mesures peuvent être prorogées pour une nouvelle durée de trois (3) mois au maximum si la mise en œuvre des procédures d'exécution n'est pas terminée, après avoir donné à la personne concernée la possibilité d'exprimer son point de vue et de proposer des solutions.

Article 323 Astreintes

Lorsque le manquement constaté est susceptible d'entraîner un préjudice grave pour un opérateur ou pour l'ensemble du marché, les mises en demeure et mesures conservatoires prononcées par l'Autorité de régulation peuvent être assorties d'une astreinte d'un montant maximum de deux pour cent du chiffre d'affaires journalier moyen hors taxes, par jour de retard à compter de la date fixée pour exécuter une mise en demeure ou mettre en œuvre les mesures conservatoires.

La base de calcul pour le montant journalier de l'astreinte est le chiffre d'affaires consolidé du dernier exercice clos à la date de la décision ou, en l'absence de chiffre d'affaires permettant de calculer le montant de l'astreinte, un montant de 2.300.000 DJF.

L'astreinte est liquidée par l'Autorité de régulation, qui en fixe le montant définitif.

Chapitre 4 : Dispositions pénales

Article 324 Application du code pénal

Les infractions établies par le présent chapitre sont réprimées dans les conditions prévues par le code pénal, notamment s'agissant de la répression de la tentative, de la complicité, du recel et pour la condamnation des personnes morales, et pour les peines complémentaires pouvant être prononcées par le juge pénal.

Article 325 Recherche et constat des infractions par l'Autorité de régulation

Outre les officiers et agents de police judiciaire, les fonctionnaires et agents assermentés de l'Autorité de régulation habilités à cet effet peuvent rechercher et constater par procès-verbal les infractions prévues par les dispositions du présent chapitre conformément aux dispositions du Chapitre 1 du présent titre.

Leurs procès-verbaux sont transmis dans les cinq (5) jours au procureur de la République. Ils font foi jusqu'à preuve contraire.

Article 326 Violation du secret des correspondances

Toute personne participant à la mise en œuvre d'un service de communications électroniques et qui viole le secret d'une correspondance ou qui, sans l'autorisation de l'expéditeur ou du destinataire, divulgue, publie ou utilise le contenu de ladite correspondance, est punie des peines prévues à cet effet par les articles 439 et 440 du Code pénal.

Article 327 Signaux ou appels de détresse faux ou trompeurs

Toute personne qui, sciemment, transmet ou met en circulation des signaux ou appels de détresse faux ou trompeurs, est punie de 3 à 12 mois d'emprisonnement et de 1.400.000 DJF d'amende.

Article 328 Utilisation frauduleuse d'un réseau de communications électroniques ouvert au public et recel

Toute personne qui utilise frauduleusement, à des fins personnelles ou non, un réseau de communications électroniques ouvert au public est puni de 1 à 5 ans d'emprisonnement et de 700.000 DJF à 7.000.000 DJFd'amende.

Toute personne qui utilise sciemment les services obtenus au moyen du délit visé à l'alinéa précédent est punie de 1 à 5 ans d'emprisonnement et de 700.000 DJF à 7.000.000 DJFd'amende.

Article 329 Utilisation frauduleuse d'indicatifs d'appel et détournement de liaisons de communications électroniques

Toute personne qui effectue des transmissions radioélectriques en utilisant sciemment un indicatif d'appel de la série internationale faux ou trompeur est punie de 90 jours à 12 mois d'emprisonnement et de 350.000 DJF à 1.400.000 DJF d'amende.

Toute personne qui effectue ou fait effectuer un détournement de liaisons de communications électroniques ou exploite des lignes de communications électroniques détournées est punie de 90 jours à 12 mois d'emprisonnement et de 350.000 DJF à 1.400.000 DJF d'amende.

Article 330 Interruption volontaire des communications électroniques

Toute personne qui, par tout moyen, cause volontairement l'interruption des communications électroniques, est punie de 1 à 3 ans d'emprisonnement et de 1.400.000 DJF à 350.000.000 DJF] d'amende.

Article 331 Interruption involontaire des communications électroniques

Toute personne qui, sans intention d'interrompre les communications électroniques, commet par maladresse ou inattention un acte ayant interrompu lesdites communications, est punie de 2 ans d'emprisonnement et de 70.000 DJF à 350.000 DJF d'amende.

Article 332 Détérioration ou rupture volontaire de câble sous-marin

Quiconque, dans les eaux territoriales ou sur le plateau continental contigu au territoire de la République de Djibouti, rompt volontairement un câble sous-marin ou lui cause ou tente de lui causer des détériorations de nature à interrompre tout ou partie des communications électroniques supportées par ce câble, est puni de 5 à 10 ans d'emprisonnement et de 70.000.000 DJF à 350.000.000 DJF d'amende.

Article 333 Détérioration ou rupture involontaire de câble sous-marin

Quiconque, dans les eaux territoriales ou sur le plateau continental contigu au territoire de la République de Djibouti, rompt par maladresse, imprudence, négligence ou inobservation des dispositions légales et réglementaires applicables, un câble sous-marin ou lui cause des détériorations de nature à interrompre tout ou partie des communications électroniques supportées par ce câble et omet d'en faire la déclaration dans les douze heures aux autorités compétentes, est puni de 1 à 12 mois d'emprisonnement et de 35.000.000 DJF à 175.000.000 DJF d'amende.

Quiconque, dans les zones maritimes visées à l'article précédent, rompt par maladresse, imprudence, négligence ou inobservation des dispositions légales et réglementaires applicables, un câble sous-marin ou lui cause des détériorations de nature à interrompre tout ou partie des communications électroniques supportées par ce câble et en fait la déclaration dans les douze heures aux autorités compétentes, est puni d'1 mois d'emprisonnement et de 14.000.000 DJF à 35.000.000 DJF d'amende.

Article 334 Perturbation des émissions radioélectriques

La perturbation des émissions radioélectriques d'un service de communications électroniques autorisé, causée par l'utilisation d'une fréquence, d'un équipement ou d'une installation radioélectrique sans posséder d'autorisation d'utilisation de fréquence radioélectrique lorsque celle-ci est requise ou dans des conditions non conformes aux conditions fixées par ladite autorisation ou aux conditions générales d'utilisation des fréquences radioélectriques fixées par l'Autorité de régulation est punie de 6 à 24 mois d'emprisonnement et de 7.000.000 DJF à 35.000.000 DJF d'amende.

Article 335 Exercice d'activité sans licence ou en violation d'une décision de suspension ou de retrait

L'établissement et/ou l'exploitation d'un réseau de communications électroniques sans licence lorsque celle-ci est requises ou en violation d'une décision de suspension ou de retrait d'une licence est puni d'1 à 5 ans d'emprisonnement et de 35.000.000 DJF à 70.000.000 DJF d'amende.

Article 336 Exercice d'activité sans autorisation ou en violation d'une décision de suspension ou de retrait

L'établissement et/ou l'exploitation d'un réseau de communications électroniques sans autorisation lorsque celle-ci est requise ou en violation d'une décision de suspension ou de retrait d'une autorisation est puni de 6 à 12 mois d'emprisonnement et de 3.500.000 DJF à 7.000.000 DJF d'amende.

Article 337 Exercice d'activité sans déclaration ou en violation d'une décision de suspension ou de retrait

L'établissement et/ou l'exploitation d'un réseau de communications électroniques sans déclaration lorsque celle-ci est requise ou en violation d'une décision de suspension ou de retrait d'une déclaration est puni de 1 à 6 mois d'emprisonnement et de 70.000 DJF à 350.000 DJF d'amende.

Article 338 Utilisation de ressources rares sans autorisation ou en violation d'une décision de suspension ou de retrait

Est puni d'1 an d'emprisonnement et de 50.000.000 DJF d'amende le fait d'utiliser :

- une ressource de numérotation sans droits d'utilisation ou en violation d'une décision de suspension ou de retrait de tels droits ;

- une fréquence radioélectrique en dehors des conditions générales fixées par l'Autorité de régulation ou de cadre prévu par des droits d'utilisation dont bénéficie l'intéressé ou qui ne lui a pas été préalablement assignée par l'Autorité de régulation ou toute autre autorité compétente.

Article 339 Exercice d'activité d'installateur d'équipements et installations radioélectriques sans agrément

Est puni d'1 an d'emprisonnement et de 3.500.000 DJF à 7.000.000 DJFd'amende le fait, sans agrément ou en violation d'une décision de suspension ou de retrait de cet agrément :

- d'installer ou faire installer des équipements ou installations radioélectriques ;

- d'exercer le métier d'installateur d'équipements ou d'installations radioélectriques.

Article 340 Non-respect des règles d'homologation et de conformité des équipements radioélectriques

Est puni d'1 an d'emprisonnement et de 3.500.000 DJF à 7.000.000 DJFd'amende le fait de :

- fabriquer ou faire fabriquer pour le marché intérieur, d'importer ou de détenir en vue de la vente ou de la distribution à titre onéreux ou gratuit, ou de mettre en vente des équipements terminaux non homologués ou de procéder à leur connexion à un réseau de communications électroniques ;

- faire de la publicité en faveur de la vente des équipements terminaux non homologués.

Article 341 Non-respect des servitudes radioélectriques

Les infractions aux dispositions relatives aux servitudes visées au Titre 7 de présent livre sont punies d'une amende de 70.000 DJF à 700.000 DJFet peuvent faire l'objet d'une astreinte fixée et liquidée par le tribunal.

Article 342 Entrave à l'exercice par l'Autorité de régulation de ses prérogatives

Est puni d'une peine de 6 mois à 10 ans d'emprisonnement et de 7.000.000 DJF à 35.000.000 DJF d'amende le fait d'entraver l'exercice par l'Autorité de régulation de ses prérogatives soit en :

14. s'opposant à l'exercice des missions confiées à ses membres ou à ses agents habilités ;

15. refusant de communiquer à ses membres ou à ses agents habilités les renseignements et documents utiles à leur mission, ou en dissimulant lesdits documents ou renseignements, ou en les faisant disparaître.

Article 343 Confiscation et destruction des matériaux et installations

En cas de condamnation pour l'une des infractions prévues au présent chapitre, le tribunal peut, en outre, prononcer la confiscation des matériels et installations constituant le réseau de communications électroniques ou permettant la fourniture du service de communications électroniques ou en ordonner la destruction aux frais du condamné et prononcer l'interdiction, pour une durée de trois années au plus, d'établir un réseau de communications électroniques ouvert au public ou de fournir un service de communications électroniques.

Article 344 Information par le procureur de la République et participation aux procédures

Le procureur de la République avise l'Autorité de régulation des poursuites engagées relatives aux infractions au présent livre et des suites qui leur sont données.

Il l'informe de la date et de 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 l'Autorité de régulation ou son représentant à déposer ses observations ou à les développer oralement à l'audience.

Livre Troisième : Cryptologie

Titre 1 Disposition générale

Article 345 Champ d'application

Le présent titre fixe le cadre légal applicable à la cryptologie en République de Djibouti.

Les dispositions du présent titre ne s'appliquent pas aux moyens de cryptologie utilisés par les missions diplomatiques et consulaires visées par la Convention de Vienne sur les relations diplomatiques de 1961 ainsi qu'à ceux relatifs à la sécurité intérieure et extérieure de l'Etat de la République de Djibouti.

Titre 2 Moyens et prestations de cryptologie

Chapitre premier : Conditions d'utilisation et de fourniture de moyens et prestations de cryptologie

Article 346 Utilisation de moyens de cryptologie

L'utilisation de moyens de cryptologie est libre.

Article 347 Fourniture, importation et exportation de moyens de cryptologie

La fourniture, l'importation et l'exportation de moyens de cryptologie assurant exclusivement des fonctions d'authentification ou de contrôle d'intégrité sont libres, sous la réserve des obligations prévues au présent code.

La fourniture ou l'importation d'un moyen de cryptologie n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité sont soumis à une déclaration préalable auprès del'Autorité nationale en charge de la Cybersécurité. Le fournisseur ou la personne procédant à l'importation tient à la disposition de l'Autorité nationale en charge de la Cybersécurité une description des caractéristiques techniques de ce moyen de cryptologie, ainsi que le code source des logiciels utilisés. Les conditions et les délais dans lesquels ces déclarations sont effectuées et dans lesquels l'autorité nationale en charge de la Cybersécuritépeut demander communication des caractéristiques du moyen, ainsi que la nature de ces caractéristiques sont déterminés par décret pris en Conseil des ministres sur proposition du Ministère en charge de l'économie numérique. Le même décret peut déterminer des catégories de moyens de cryptologie dont les caractéristiques techniques ou les conditions d'utilisation sont telles que, au regard des intérêts de la

défense nationale et de la sécurité intérieure ou extérieure de l'Etat, leur fourniture, ou leur importation peuvent être dispensés de toute formalité préalable.

L'exportation de moyens de cryptologie n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité est soumise à l'autorisation de l'Autorité nationale en charge de la Cybersécurité. Le fournisseur ou la personne procédant à l'exportation tient à la disposition de l'Autorité nationale en charge de la Cybersécurité une description des caractéristiques techniques de ce moyen de cryptologie, ainsi que le code source des logiciels utilisés. Les conditions et les délais dans lesquels l'autorisation est effectuée et dans lesquels l'Autorité nationale en charge de la Cybersécurité peut demander communication des caractéristiques du moyen, ainsi que la nature de ces caractéristiques sont déterminés par décret pris en Conseil des ministres sur proposition du ministère en charge de l'économie numérique. Le même décret peut déterminer des catégories de moyens de cryptologie dont les caractéristiques techniques ou les conditions d'utilisation sont telles que, au regard des intérêts de la défense nationale et de la sécurité intérieure ou extérieure de l'Etat, leur fourniture, ou leur exportation peuvent être dispensés de toute formalité préalable.

Article 348 Fourniture de prestations de cryptologie

Les prestations de cryptologie sont soumises à une déclaration préalable auprès de l'Autorité nationale en charge de la Cybersécurité.

Les conditions et les délais dans lesquels la déclaration préalable est effectuée et dans lesquels l'Autorité nationale en charge de la Cybersécurité peut demander communication des caractéristiques de la prestation de cryptologie sont déterminés par décret pris en Conseil des ministres sur proposition du Ministère en charge de de l'économie numérique. Le même décret peut déterminer des catégories de prestations de de cryptologie dont les caractéristiques techniques ou les conditions d'utilisation sont telles que, au regard des intérêts de la défense nationale et de la sécurité intérieure ou extérieure de l'Etat, leur fourniture, ou leur importation peuvent être dispensés de toute formalité préalable.

Sauf à démontrer qu'elles n'ont commis aucune faute intentionnelle ou négligence, les personnes fournissant des prestations de cryptologie sont responsables au titre de ces prestations, nonobstant toute stipulation contractuelle contraire, du préjudice causé aux personnes leur confiant la gestion de leurs conventions secrètes en cas d'atteinte à l'intégrité, à la confidentialité ou à la disponibilité des données transformées à l'aide de ces conventions.

Chapitre 2 : Recherche des infractions

Article 349 Habilitation à la recherche d'infractions

Outre les officiers et agents de police judiciaire agissant conformément aux dispositions du code de procédure pénale et, dans leur domaine de compétence, les agents des douanes agissant conformément aux dispositions du code des douanes, les agents habilités à cet effet par l'autorité nationale en charge de la cybersécurité et assermentés dans des conditions fixées par décret pris en Conseil des ministres peuvent rechercher et constater par procès-verbal les infractions aux dispositions du Chapitre Premier du présent titre et des textes pris pour leur application.

Cette habilitation ne dispense pas de l'application des dispositions définissant les procédures autorisant l'accès aux secrets protégés par la loi et assurant la protection des libertés individuelles.

Article 350 Pouvoir d'enquête, droit de visite, recueil de documents

Les agents habilités à cet effet ont accès, dans les conditions prévues par le code de procédure pénale, aux moyens de transport, lieux, terrains ou locaux à usage professionnel, à l'exclusion des parties de ceux-ci affectées à un usage d'habitation, en vue de rechercher et de constater les infractions, demander la communication de tous documents professionnels et en prendre copie, recueillir, sur convocation ou sur place, les renseignements et justifications.

Le procureur de la République en est préalablement informé.

En cas d'opposition du responsable des lieux, ou lorsqu'il s'agit de lieux mentionnés au premier alinéa affectés à un usage d'habitation, la visite ne peut se dérouler qu'avec l'autorisation du président du Tribunal de première instance ou du juge délégué par lui. Toutefois, lorsque l'urgence, la gravité des faits à l'origine du contrôle ou le risque de destruction ou de dissimulation de documents le justifie, la visite peut avoir lieu sans que le responsable des locaux en ait été informé, sur autorisation préalable du président du Tribunal de première instance. Dans ce cas, le responsable des lieux ne peut s'opposer à la visite. La visite s'effectue sous l'autorité et le contrôle du président du Tribunal de première instance ou du juge délégué par lui, en présence de l'occupant des lieux ou de son représentant qui peut se faire assister d'un conseil de son choix ou, à défaut, en présence de deux témoins qui ne sont pas placés sous l'autorité des personnes chargées de procéder au contrôle.

Le président du Tribunal de Première Instance est saisi à la requête du président de l'Autorité de régulation. Il statue par ordonnance motivée dans les conditions prévues par la loi. L'ordonnance est exécutoire au seul vu de la minute. Elle mentionne que le juge ayant autorisé la visite peut être saisi à tout moment d'une demande de suspension ou d'arrêt de cette visite et indique les voies et délais de recours.

Article 351 Saisies

Les agents habilités à cet effet peuvent, avec l'autorisation et sous le contrôle du président du Tribunal de première instance ou du juge délégué par lui saisi dans les conditions fixées par l'Article 350 , procéder à la saisie des moyens de cryptologie. La demande de l'autorisation précitée doit comporter tous les éléments d'information de nature à justifier la saisie. Les matériels et logiciels saisis sont immédiatement inventoriés. A titre de mesure conservatoire, les fonctionnaires et agents assermentés de l'Autorité de régulation habilités à cet effet peuvent procéder à la mise sous scellés des matériels et équipements dès la constatation de l'infraction.

Article 352 Établissement de procès-verbaux

Il est dressé procès-verbal des contrôles, vérifications, visites et saisies effectuées par les agents habilités conformément aux dispositions du présent Chapitre.

Leurs procès-verbaux sont transmis dans les cinq (5) jours aux personnes intéressées et, le cas échéant, au président du Tribunal de Première Instance ou au juge délégué par lui qui a autorisé la visite et/ou la saisie. Ils font foi jusqu'à preuve contraire.

Chapitre 3 : Sanctions

Section 1 : Sanctions administratives

Article 353 Interdiction de mise en circulation et retrait

Lorsqu'un fournisseur de moyens de cryptologie, même à titre gratuit, ne respecte pas les obligations auxquelles il est assujetti en application des dispositions du Chapitre Premier du présent titre, l'Autorité nationale en charge de la Cybersécuritépeut, après avoir mis l'intéressé à même de présenter ses observations, prononcer l'interdiction de mise en circulation du moyen de cryptologie concerné.

L'interdiction de mise en circulation est applicable sur l'ensemble du territoire national. Elle emporte en outre pour le fournisseur l'obligation de procéder au retrait :

1. Auprès des diffuseurs commerciaux et des distributeurs, des moyens de cryptologie dont la mise en circulation a été interdite ;

2. Des matériels constituant des moyens de cryptologie dont la mise en circulation a été interdite et qui ont été acquis à titre onéreux, directement ou par l'intermédiaire de diffuseurs commerciaux ou de distributeurs.

Le moyen de cryptologie concerné pourra être remis en circulation dès que les obligations antérieurement non respectées auront été satisfaites, dans les conditions prévues au Chapitre Premier du présent titre.

Section 2 : Dispositions pénales

Article 354 Violation des conditions de fourniture

Le fait de fournir, importer ou exporter des moyens de cryptologie ou de fournir des prestations de cryptologie en violation des conditions fixées par les dispositions du chapitre premier du présent titre est puni d'une peine maximum de 6 mois à 5 ans d'emprisonnement et d'une peine d'amende maximum de 700.000 DJF à 3.500.000 DJF.

Article 355 Entrave au déroulement des enquêtes

Le fait de faire obstacle au déroulement des enquêtes prévues par les dispositions du Chapitre 2 du présent titre ou de refuser de communiquer habilités les renseignements et documents y afférant, ou de dissimulant lesdits renseignements ou documents ou de les faire faisant disparaître est puni d'une peine maximum de 1 à 5 ans d'emprisonnement et d'une peine d'amende maximum de 700.000 DJF à 14.000.000 DJF.

Article 356 Non-respect de décisions d'interdiction de mise en circulation

Le fait de vendre ou de louer un moyen de cryptologie ayant fait l'objet d'une interdiction de mise en circulation conformément à l'article relatif à l'interdiction de mise en circulation est puni de 1 à 5 ans d'emprisonnement et de 700.000 DJF à 14.000.000 DJF d'amende.

Article 357 Refus de communication d'une convention de déchiffrement

Le fait, pour quiconque ayant connaissance de la convention secrète de déchiffrement d'un moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit, de refuser de communiquer ladite convention aux autorités judiciaires ou de la mettre en œuvre, sur réquisition de ces autorités, est puni d'une peine d'emprisonnement maximum de 3 ans et d'une amende maximum de 700.000 DJF à 14.000.000DJF.

Si le refus est opposé alors que la remise ou la mise en œuvre de la convention aurait permis d'éviter la commission d'un crime ou d'un délit ou d'en limiter les effets, les peines visées à l'alinéa précédent sont portées au double.

Article 358 Circonstance aggravante d'utilisation d'un moyen de cryptologie

Lorsqu'un moyen de cryptologie a été utilisé pour préparer ou commettre un crime ou un délit, ou pour en faciliter la préparation ou la commission, le maximum de la peine privative de liberté encourue est relevé ainsi qu'il suit :

1. Il est porté à la réclusion criminelle à perpétuité lorsque l'infraction est punie de vingt ans de réclusion criminelle ;

2. Il est porté à vingt ans de réclusion criminelle lorsque l'infraction est punie de quinze ans de réclusion criminelle ;

3. Il est porté à quinze ans de réclusion criminelle lorsque l'infraction est punie de dix ans de réclusion criminelle ou de dix ans d'emprisonnement ;

4. Il est porté à dix ans d'emprisonnement lorsque l'infraction est punie de cinq ans d'emprisonnement ;

5. Il est porté à cinq ans d'emprisonnement lorsque l'infraction est punie de trois ans d'emprisonnement ;

6. Il est porté au double lorsque l'infraction est punie de deux ans d'emprisonnement au plus.

Les dispositions du présent article ne sont toutefois pas applicables à l'auteur ou au complice de l'infraction qui, à la demande des autorités judiciaires ou administratives, leur a remis la version en clair des messages chiffrés ainsi que les conventions secrètes nécessaires au déchiffrement.

Livre Quatrième : Commerce électronique

Titre 1 Régime des activités de commerce électronique

Chapitre 1 : Champ d'application

Article 359 Champ d'application

Les dispositions du présent livre s'appliquent à toute commande, contrat ou transaction conclus en ligne ou par voie électronique en vue de la fourniture de biens ou services, ainsi qu'à toute activité de commerce électronique exercée sur le territoire de la République de Djibouti ou à destination des utilisateurs établis sur le territoire de la République de Djibouti.

Une activité de commerce électronique ou une offre de biens ou services est considérée comme à destination des utilisateurs établis sur le territoire de la République de Djibouti, si elle inclut un signe distinctif ou caractéristique de la République de Djibouti, de ses ressortissants ou de ses résidents.

Par ailleurs, les messages publicitaires et offres proposées sont considérés comme à destination des utilisateurs établis sur le territoire de la République de Djibouti en fonction de leur contenu, de la langue, de la monnaie et du nom de domaine utilisés.

Sans préjudice des dispositions librement convenues entre les parties à un contrat électronique, les dispositions du présent Livre sont applicables dès lors qu'un contrat est conclu entre un professionnel et un consommateur.

Article 360 Exclusions

Sont exclus du champ d'application du présent livre :

1. les jeux d'argent, y compris sous forme de paris et de loteries, légalement autorisés ;
2. les activités de représentation et d'assistance en justice ;
3. les activités exercées par les notaires.

Article 361 Dérogations

Les contrats conclus entre professionnels peuvent déroger aux dispositions du présent Livre, pour autant que ce choix n'ait pas pour objet ou pour effet de :

1. déroger aux dispositions d'ordre public djiboutien ;

2. priver un consommateur de la protection que lui assurent les dispositions impératives de la loi;

3. déroger aux dispositions impératives régissant les transactions ou activités soumises à un régime particulier, dont notamment :

    i. en matière immobilière à l'exception des contrats de location immobilière ;

    ii. en matière d'assurance ;

    iii. en matière de droit de la famille et des successions ;

    iv. en matière de sûretés et garanties fournies par des personnes agissant à des fins qui n'entrent pas dans le cadre de leur activité professionnelle ou commerciale ;

    v. toutes autres matières pour lesquelles la loi requiert l'intervention des tribunaux, des autorités publiques ou de professions exerçant une autorité publique.

Chapitre 2 : Obligations

Article 362 Obligation générale d'information

Sans préjudice des autres obligations d'information prévues par le Livre V ainsi que par les textes législatifs et réglementaires en vigueur, toute personne physique ou morale exerçant une activité soumise aux dispositions du présent Livre est tenue d'assurer à ceux à qui est destinée la fourniture de biens ou la prestation de services un accès facile, direct et permanent utilisant un standard ouvert aux informations suivantes :

1. s'il s'agit d'une personne physique, ses nom et prénoms et, s'il s'agit d'une personne morale, sa raison sociale ;

2. l'adresse où elle est établie, son adresse de courrier électronique, ainsi que des coordonnées téléphoniques permettant d'entrer effectivement en contact avec elle ;

3. son numéro d'immatriculation au Registre du Commerce, son capital social et l'adresse de son siège social ;

4. si elle est assujettie à la TVA, le numéro d'identification fiscale correspondant ;

5. si son activité est soumise à un régime d'autorisation, la référence de l'autorisation, le nom et l'adresse de l'autorité l'ayant délivrée ;

6. si elle est membre d'une profession réglementée, la référence aux règles professionnelles applicables, son titre professionnel, l'Etat dans lequel il a été attribué, ainsi que le nom de l'ordre ou de l'organisme professionnel auprès duquel elle est inscrite.

Toute personne physique ou morale exerçant une activité soumise aux dispositions du présent Livre doit, même en l'absence d'offre de contrat, dès lors qu'elle mentionne un prix, indiquer celui-ci de manière claire et non ambiguë, et notamment si les taxes et les frais de livraison sont inclus.

Article 363 Obligation de traçabilité

Tout fournisseur de services en ligne dont l'activité consiste à mettre en relation un professionnel exerçant une activité de commerce électronique et un consommateur final, est tenu d'obtenir du professionnel les informations préalables énoncées à l'Article 362 ainsi qu'une déclaration du professionnel selon laquelle ce dernier fournit des produits ou services conformes aux textes législatifs et réglementaires en vigueur. Le fournisseur de services en ligne est tenu de fournir les efforts raisonnables nécessaires à la vérification des informations fournies par le professionnel susvisé.

En cas d'information incomplète ou erronée, le fournisseur de services en ligne est tenu de solliciter les informations manquantes au professionnel. Le fournisseur de services en ligne suspend l'accès du professionnel aux services fournis tant que les informations manquantes ne lui ont pas été communiquées.

Le fournisseur de services en ligne conserve les informations fournies par le professionnel pendant toute la durée de leur relation contractuelle ou commerciale.

Article 364 Obligation de vigilance relative aux contenus illicites

Tout professionnel exerçant une activité de commerce électronique, et tout fournisseur de services en ligne, sont tenus à une obligation générale de vigilance relative aux contenus illicites postés ou proposés dans le cadre de leur activité, par eux-mêmes ou par tout utilisateur de leurs services.

A ce titre, ils sont tenus d'informer sans délai les services de police de la République de Djibouti, de toute activité illégale, illicite ou suspecte dont ils pourraient avoir connaissance.

Article 365 Justification de toute décision de retrait ou de restriction d'accès à un contenu illicite

Tout fournisseur de services en ligne dont l'activité consiste à mettre en relation un professionnel exerçant une activité de commerce électronique et un consommateur final, est tenu de restreindre l'accès ou de supprimer tout contenu illicite transmis ou posté par un professionnel du commerce électronique utilisant ses services.

Toute décision de retrait ou de restriction d'accès au contenu illicite est justifiée par le fournisseur de services en ligne auprès du professionnel utilisant ses services et exerçant une activité de commerce électronique visant le consommateur final.

Article 366 Obligation de mise à disposition des stipulations contractuelles et modalités de conclusion du contrat

Toute personne qui propose, à titre professionnel, par voie électronique, la fourniture de biens ou la prestation de services, met à disposition les stipulations contractuelles applicables directement ou indirectement, d'une manière qui permette leur conservation et leur reproduction conformément aux textes législatifs et réglementaires en vigueur.

Ces informations doivent être présentées de façon claire, lisible et non-équivoque et comprennent notamment :

1. les différentes étapes à suivre par l'utilisateur pour conclure le contrat en ligne ;
2. les langues proposées pour la conclusion du contrat ;
3. les dispositions relatives à la protection des données à caractère personnel ;
4. les moyens techniques appropriés permettant à l'utilisateur d'identifier les erreurs commises dans la saisie des données et de les corriger avant la conclusion du contrat ;
5. le mode de confirmation de l'acceptation de l'offre ;
6. les conséquences de l'absence de confirmation des informations communiquées par l'utilisateur ;
7. les informations relatives aux restrictions, limitations et/ou aux conditions liées à la conclusion du contrat, telles que l'accord obligatoire d'un parent ou d'un tuteur, le cas échéant ;
8. les conditions de conclusion du contrat ;
9. les conditions de résiliation du contrat pour les contrats à durée indéterminée ou d'une durée supérieure à un (1) an ;
10. la durée minimale du contrat pour les contrats portant sur la fourniture de produits ou services périodiquement ou à long terme ;
11. les conditions de livraison et frais de livraison ;
12. la date à laquelle le fournisseur s'engage à livrer les biens ou à fournir les services ;

13. les conséquences d'une inexécution ou d'une mauvaise exécution des obligations du fournisseur ;

14. les modalités prévues par le fournisseur pour le traitement des réclamations ;

15. le numéro de téléphone, ainsi que l'adresse électronique et postale du fournisseur en vue d'éventuelles réclamations ;

16. le cas échéant, les informations relatives aux procédures extrajudiciaires de réclamation et de recours auxquelles le fournisseur est soumis, et les conditions d'accès à celles-ci ;

17. l'existence ou l'absence d'un droit de rétractation et ses conditions d'exercice ;

18. les modalités de retour, d'échange et de remboursement des biens ;

19. le cas échéant, les informations relatives à l'assistance après-vente, le service après-vente et les conditions y afférentes ;

20. le cas échéant, les informations relatives à la nature et l'étendue des garanties commerciales ;

21. les informations relatives aux garanties légales de conformité, garanties légales des vices cachés et garanties légales d'éviction ;

22. les modalités d'archivage du contrat ainsi que les conditions d'accès au contrat archivé ;

23. les modalités de consultation des certificats de signature et de cachets électroniques ;

24. les règles professionnelles et commerciales ou codes de conduite auxquels l'auteur de l'offre entend se soumettre, ainsi que les moyens de les consulter.

Article 367 Obligation d'information sur les caractéristiques des biens et services

Toute personne physique ou morale exerçant une activité soumise aux dispositions du présent Livre doit, avant la conclusion de tout contrat, assurer et maintenir un accès facile, direct et permanent sur support durable, à toute information portant sur les caractéristiques des biens ou services proposés.

Ces informations sont présentées de façon claire, lisible, non-équivoque et comprennent notamment :

1. les caractéristiques essentielles du bien ou du service ;

2. les caractéristiques techniques du bien ou du service ;

3. les informations relatives au mode d'emploi et conditions d'utilisation du bien ou du service;

4. les mises en garde relatives à la sécurité et à la santé liées au bien ou au service ;

5. s'il s'agit d'un contenu numérique, ses fonctionnalités, et s'il y a lieu, les mesures de protections applicables et toute interopérabilité du contenu numérique avec certains matériels ou logiciels dont le fournisseur a ou devrait raisonnablement avoir connaissance.

Article 368 Obligation d'information sur la dangerosité des biens et services

Tout bien ou service dangereux pour la santé humaine ou animale ou pour l'environnement est accompagné d'un manuel d'instructions, comprenant des avertissements clairs et facilement visibles, afin de permettre une utilisation dans des conditions de sécurité maximales.

Article 369 Obligation d'information sur le prix des biens et services

Sous peine de nullité, toute personne physique ou morale exerçant une activité soumise aux dispositions du présent Livre doit, avant la conclusion de tout contrat, assurer et maintenir un accès facile, direct et permanent sur support durable, à toutes informations portant sur le prix des biens et services proposés.

Ces informations sont présentées de façon claire, lisible et non-équivoque, et comprennent notamment :

1. le prix du bien ou du service toutes taxes comprises et s'il inclut ou non les frais de livraison ;

2. le cas échéant, les frais de livraison ainsi que les assurances proposées ;

3. la durée de validité de l'offre ;

4. les modalités, conditions et méthodes de paiement ;

5. le cas échéant, les facilités de paiement proposées ;

6. la monnaie de facturation du bien ou du service ;

7. le cas échéant, les coûts d'utilisation des services en ligne ;

8. le cas échéant, les coûts d'utilisation des moyens de communications électroniques lorsqu'ils sont calculés sur une autre base que les tarifs en vigueur, notamment s'agissant des numéros surtaxés ;

9. le cas échéant, l'existence d'autres coûts normalement dus par l'utilisateur, non-perçus par le fournisseur et/ou non imposés par celui-ci.

Toutes les informations faisant référence à des coûts prévus au présent article doivent indiquer la monnaie utilisée.

Article 370 Obligation d'information sur la disponibilité des biens et services

En cas d'indisponibilité du bien ou du service en ligne, la personne qui propose le bien ou la prestation de service par voie électronique doit en informer l'autre partie sans délai et au moins vingt-quatre (24) heures avant la date de livraison prévue au contrat.

Le cas échéant, la personne qui propose le bien ou la prestation de service par voie électronique rembourse à l'autre partie l'intégralité des sommes déjà perçues.

Chapitre 3 : Responsabilité et charge de la preuve

Article 371 Responsabilité contractuelle

Toute personne physique ou morale exerçant une activité soumise aux dispositions du présent livre ou partie à un contrat encadré par les dispositions du présent livre est responsable de plein droit de la bonne exécution des obligations résultant du contrat, que ces obligations soient à exécuter par elle-même ou par des tiers, sans préjudice de son droit de recours contre ceux-ci.

Toutefois, elle peut s'exonérer de tout ou partie de sa responsabilité en apportant la preuve que l'inexécution ou la mauvaise exécution du contrat est imputable, soit à l'autre partie ou à un tiers, soit à un cas de force majeure.

Article 372 Charge de la preuve

La charge de la preuve de l'existence d'une information préalable, d'une confirmation des informations communiquées, du respect des délais et du consentement de l'utilisateur incombe la personne qui propose le bien ou la prestation de service par voie électronique.

Titre 2 Ecrits et contrats conclus par voie électronique

Chapitre 1 : Dispositions modificatives

Article 373 Contrat conclu par échange de courriers électroniques

En complément de l'article 1270 du code civil, lorsqu'il est conclu par voie électronique, le contrat n'est valable que si le destinataire de l'offre a eu la possibilité de vérifier le détail de sa commande et son prix total et de corriger d'éventuelles erreurs avant de confirmer celle-ci pour exprimer son acceptation définitive. Toutefois cette obligation n'est pas applicable aux contrats conclus exclusivement par échange de courriers électroniques.

L'auteur de l'offre doit accuser réception sans délai injustifié, par voie électronique, de la commande qui lui a été adressée. Toutefois cette obligation n'est pas applicable aux contrats conclus exclusivement par échange de courriers électroniques.

La commande, la confirmation de l'acceptation de l'offre et l'accusé de réception sont considérés comme reçus lorsque les parties auxquelles ils sont adressés peuvent y avoir accès.

Article 374 Etablissement et conservation d'un écrit sous forme électronique pour la validité d'un contrat

En complément de l'article 1241 du code civil, lorsqu'un écrit est exigé pour la validité d'un contrat, que ce soit sous signature privée ou par acte authentique, il peut être établi et conservé sous forme électronique, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir non seulement l'intégrité mais encore le lien entre la signature électronique et l'acte auquel elle s'attache.

Une signature électronique a le même effet juridique qu'une signature manuscrite selon les conditions et modalités prévues par la loi.

Article 375 Présomption de fiabilité d'un procédé de signature électronique

En complément de l'article 1596 du code civil, la signature nécessaire à la perfection d'un acte juridique identifie son auteur. Elle manifeste son consentement aux obligations qui découlent de cet acte. Quand elle est apposée par un officier public, elle confère l'authenticité à l'acte. Lorsqu'elle est électronique, elle a le même effet juridique qu'une signature manuscrite selon les conditions et modalités prévues par la loi.

Chapitre 2 : Dispositions complémentaires

Section 1 : L'écrit électronique

Article 376 Equivalence des exigences de lisibilité et de présentation de l'écrit électronique

Lorsque l'écrit sur papier est soumis à des exigences particulières de lisibilité ou de présentation, l'écrit électronique doit répondre à des exigences équivalentes.

Article 377 Version électronique originale

Tout écrit ou document électronique satisfait aux obligations de présentation ou de conservation des informations qu'ils contiennent sous leur forme originale dès lors que :

1) l'intégrité et l'exactitude des informations générées sont garanties et maintenues de manière fiable ;

2) il est possible de reproduire avec exactitude l'intégralité des informations telles qu'elles ont été générées pour la première fois.

L'exigence d'intégrité visée au présent article est satisfaite dès lors que les informations sont demeurées complètes et inchangées, à l'exception d'ajouts mineurs liés à l'acheminement ou au stockage des informations.

Article 378 Actes authentiques dressés sur support électronique

L'acte authentique peut être dressé sur support électronique, sous réserve qu'il soit établi et conservé dans des conditions de nature à en garantir son intégrité, et que la personne dont il émane puisse être dûment identifiée.

Article 379 Valeur de l'écrit électronique produit en justice

L'écrit électronique produit en justice est admis au même titre que l'écrit sur support papier et a la même force probante que celui-ci, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité.

Article 380 Effectivité de la remise d'un écrit électronique

La remise d'un écrit sous forme électronique est effective lorsque le destinataire, après en avoir pris connaissance, en accuse réception par tout moyen, y compris par voie électronique.

Section 2 : Formation du contrat par voie électronique

Article 381 Droit de mise à disposition d'informations par voie électronique

Les informations qui sont demandées en vue de la conclusion d'un contrat ou celles qui sont adressées au cours de son exécution peuvent être transmises par moyen électronique si leurs destinataires ont accepté l'usage de ce moyen.

L'utilisation des communications électroniques est présumée recevable sauf si le bénéficiaire a déjà exprimé sa préférence pour un autre moyen de communication.

Article 382 Transmission d'informations nécessaires à la conclusion ou l'exécution du contrat par courrier électronique

Les informations demandées en vue de la conclusion d'un contrat en ligne ou celles qui sont adressées ou échangées au cours de son exécution peuvent être transmises par voie électronique si le destinataire a accepté l'usage de ce procédé.

Article 383 Envoi d'informations à un professionnel par voie électronique

Les informations destinées à un professionnel peuvent lui être adressées par courrier électronique, si ce dernier a communiqué son adresse électronique.

Article 384 Formulaires mis à disposition par voie électronique

Si les informations destinées à un professionnel doivent être portées sur un formulaire, la forme électronique de ce formulaire est mise à disposition de la personne devant le remplir.

Article 385 Valeur et contenu de l'offre portant sur des contenus numériques téléchargés

Pour les contenus numériques téléchargés, l'offre doit indiquer :

1. les caractéristiques du système d'exploitation ou de l'équipement nécessaire pour utiliser de manière efficace le contenu téléchargé ;

2. le temps approximatif et le coût de téléchargement éventuel du contenu, et le cas échéant, les modalités et conditions du contrat de licence ;

3. les caractéristiques techniques pour reprendre le téléchargement d'un contenu interrompu ;

4. le cas échéant, le nom du directeur de publication.

Sans préjudice des conditions de validité mentionnées dans l'offre, l'auteur reste engagé par elle tant qu'elle est accessible par l'utilisateur.

Article 386 Echange d'informations et personnes frappées d'incapacité juridique

Les informations faisant l'objet de la présente section sont fournies sans préjudice des dispositions relatives à la protection des personnes frappées d'incapacité juridique, notamment les mineurs et les majeurs incapables.

Article 387 Conservation et accès aux contrats conclus par voie électronique

Tout contrat conclu par voie électronique doit être conservé pour une durée de dix (10) ans à compter de la livraison du bien ou de la fourniture du service.

Chapitre 3 : Preuve électronique

Article 388 La preuve électronique

Les dispositions établies au présent titre s'appliquent sans préjudice des dispositions du Code civil régissant la preuve par écrit, notamment l'article 1595 établissant l'équivalence de force probante entre un écrit sous forme électronique et un écrit sous forme papier.

Titre 3 Services de confiance électronique

Chapitre 1 : Dispositions générales

Section 1 : Régime juridique des prestataires de services de confiance

Article 389 Déclaration des prestataires de services de confiance

Tout prestataire de services de confiance établi en République de Djibouti et toute personne qui a l'intention d'exercer une activité de prestataire de services de confiance soumet à l'Organe en charge de la certification racine une déclaration, selon les modalités que cette dernière indique, qui comprend les informations suivantes :

1. s'il s'agit d'une personne physique, ses nom et prénoms et, s'il s'agit d'une personne morale, sa raison sociale et sa dénomination sociale ainsi que le nom et prénom de son dirigeant social;
2. l'adresse où il est établi, son adresse de courrier électronique, ainsi que des coordonnées téléphoniques permettant d'entrer effectivement en contact avec elle ;

3. son numéro d'immatriculation au Registre du Commerce, son capital social et l'adresse de son siège social ;

4. s'il est assujetti à la TVA, le numéro d'identification fiscale correspondant ;

5. un justificatif de souscription à une police d'assurance couvrant de manière efficace les dommages liés à son activité ;

6. Une description technique des dispositifs qu'il envisage de proposer ;

7. Une description circonstanciée des procédures de sécurité qu'il envisage d'adopter pour protéger ses locaux et équipements informatiques ;

8. Les documents permettant de justifier les moyens matériels, financiers et humains lui permettant de fournir un service de confiance.

La déclaration visée au premier alinéa est transmise par lettre recommandée, par voie électronique ou en mains propres selon les modalités décrites par l'Organe en charge de la certification racine et intervient avant le début de l'activité du prestataire de services de confiance ou dans le mois suivant l'entrée en vigueur du présent Code.

L'Organe en charge de la certification racine délivre aux prestataires de services de confiance un récépissé de déclaration, dans les mêmes formes, dans les cinq (5) jours ouvrables suivant leur déclaration.

Article 390 Demande d'octroi du statut qualifié

Toute personne physique ou morale désirant fournir un ou plusieurs services de confiance qualifiés doit au préalable demander l'octroi du statut qualifié auprès de l'Organe en charge de la certification racine.

Les demandes sont adressées par lettre recommandée ou par voie électronique sur le site de l'Organe en charge de la certification racine. Il en est accusé réception dans les mêmes formes.

A défaut, les demandes peuvent être déposées directement auprès du bureau de l'Organe en charge de la certification racine contre décharge.

Le dossier contient obligatoirement les documents suivants :

1. une fiche de renseignement fournie par l'Organe en charge de la certification racine dûment remplie et signée par le demandeur ;

2. les documents justificatifs des moyens matériels, financiers et humains du demandeur ;

3. une description technique des dispositifs de création, de certification, de validation et de conservation des signatures électroniques envisagés ;

4. une description détaillée des procédures de sécurité adoptées pour la sécurisation des locaux et des équipements informatiques.

Article 391 Critères d'acceptation de la demande de qualification

Les critères d'acceptation de la demande de qualification sont :

1. le dossier de demande de qualification est complet, et transmis selon les modalités prévues à l' Article 390 ;
2. le service répond aux besoins de la sécurité nationale ou de sécurité dans les transactions électroniques au sein du territoire national ;
3. la qualification demandée est cohérente avec les objectifs et fonctions de sécurité du service de confiance fixés par l'Organe en charge de la certification racine ;
4. le commanditaire est en mesure de respecter l'ensemble de ses engagements pris dans le dossier de demande de qualification.

L'Organe en charge de la certification racine vérifie que le prestataire de services de confiance et les services de confiance qu'il fournit respectent les exigences fixées par le présent Code, en particulier les exigences en ce qui concerne les prestataires de services de confiance qualifiés et les services de confiance qualifiés qu'ils fournissent.

Article 392 Instruction

L'instruction de la demande de qualification vise à vérifier que l'ensemble des critères d'acceptation définis à l'Article 391 sont respectés. Dans le cadre de l'instruction de la demande de qualification, le chargé de qualification peut inviter le commanditaire à soutenir sa demande de qualification au cours d'une ou plusieurs réunions ou lui demander de modifier ou compléter son dossier de demande de qualification.

L'instruction est finalisée dans un délai d'un (1) mois à compter de la date de soumission du dossier de demande de qualification, renouvelable par période d'un (1) mois pour des raisons dûment justifiées.

Article 393 Evaluation

Conformément à la stratégie d'évaluation définie par l'Organe en charge de la certification racine, un évaluateur évalue la robustesse du service de confiance et sa conformité au référentiel d'exigences fixé par l'Organe en charge de la certification racine.

L'Organe en charge de la certification racine peut-être l'évaluateur visé à l'alinéa précédent et peut le cas échéant s'appuyer sur l'expertise des administrations compétentes, un prestataire d'audit de la sécurité des systèmes d'information qualifié ou un centre d'évaluation agréé par l'Organe en charge de la certification racine.

Article 394 Octroi du statut de prestataire de services de confiance qualifié

Le directeur général de l'Organe en charge de la certification racine, sur proposition du chargé de qualification, accepte la demande de qualification lorsque l'ensemble des critères d'acceptation définis à l'Article 391 sont respectés. Lorsqu'une décision d'acceptation de la demande de qualification est prononcée, le prestataire de service de confiance obtient le statut « en cours de qualification ».

Le directeur général de l'Organe en charge de la certification racine, sur proposition du chargé de qualification, refuse la demande de qualification lorsqu'au moins un des critères définis à l'Article 391 n'est pas respecté. Les motifs du refus de la demande de qualification sont exposés dans la notification de la décision.

L'Organe en charge de la certification racine est tenue de répondre à la demande formulée dans un délai maximum de quarante-cinq (45) jours à compter de la réception du dossier complet et notifie la décision d'acceptation ou la décision de refus de la demande de qualification au commanditaire selon les modalités qu'elle prévoit.

Le silence de l'Organe en charge de la certification racine vaut acceptation.

Article 395 Contenu d'une décision d'octroi du statut de prestataire de services de confiance qualifié

Les conditions et éventuelles restrictions d'utilisation d'un service sont fixées par l'Organe en charge de la certification racine.

Pour chaque service qualifié, l'Organe en charge de la certification racine définit et tient à jour un niveau de recommandation, représentant ses prescriptions d'utilisation du service au regard de son niveau de sécurité et de pérennité. Ce niveau évolue dans le temps, en fonction d'éléments issus du suivi de la qualification, par exemple l'identification de non-conformités au référentiel d'exigences fixés par l'Organe en charge de la certification racine ou des évolutions de l'état de l'art ou de l'offre de service de confiance du prestataire de service de confiance.

Article 396 Redevances dues pour le statut qualifié

Un arrêté du Ministre chargé de l'économie numérique fixe le montant des redevances dues à l'Organe en charge de la certification racine par les prestataires de services de confiance qualifiés pour l'octroi du statut qualifié.

Article 397 Caractère personnel et durée de l'attribution du statut qualifié

Le statut qualifié est octroyé à titre personnel. Il ne peut être ni cédé ni transféré à un tiers sans autorisation expresse de l'Organe en charge de la certification racine.

Le statut qualifié est attribué pour dix (10) ans à compter de la date de la réponse formulée par l'Organe en charge de la certification racine précisant l'octroi du statut qualifié.

Le prestataire de services de confiance peut demander le renouvellement de la qualification en déposant une nouvelle demande de qualification.

Article 398 Cessation des activités des prestataires de services de confiance qualifiés

Le prestataire de services de confiance qualifié informe l'Organe en charge de la certification racine, dans un délai raisonnable, de son intention de cesser ses activités ou de tout fait qui pourrait conduire à la cessation de ses activités.

Dans ce cas, il s'assure de la reprise de ses activités par un autre prestataire de services de confiance garantissant un niveau de qualité et de sécurité au moins équivalent. En l'absence de repreneur, le prestataire révoque, sous réserve d'un préavis de deux (2) mois, les certificats octroyés à ses titulaires.

Le prestataire de services de confiance qui cesse ses activités pour des raisons indépendantes de sa volonté ou en cas de faillite, en informe immédiatement l'Organe en charge de la certification racine. Il procède, le cas échéant, à la révocation des certificats délivrés.

Article 399 Liste des prestataires de services de confiance qualifiés

Les prestataires de services de confiance qualifiés sont inscrits sur une liste de confiance, tenue à jour par l'Organe en charge de la certification racine et qui fait l'objet, à la fin de chaque année, d'une publication au Journal officiel et sur le site internet de l'Organe en charge de la certification racine.

Cette liste mentionne pour chaque prestataire de services de confiance qualifié :

1. L'identité du prestataire de services de confiance qualifié :

    - Pour une personne physique : son nom et son prénom ;

    - Pour une personne morale : sa raison sociale, sa dénomination sociale, le nom et lieu du registre et son numéro d'inscription ;

2. Ses coordonnées : adresse de l'endroit où elle est établie, le cas échéant adresse de son siège social, adresse de courrier électronique ;

3. Les services de confiance qu'il fournit et son statut ;

4. La référence de la décision de qualification ;

5. La date de début de la qualification du prestataire de services de confiance.

Article 400 Confidentialité

Les informations échangées dans le cadre de la qualification d'un service de confiance présentent un caractère confidentiel.

L'Organe en charge de la certification racine traite ces informations selon des règles de protection adéquates. Tous les documents confidentiels échangés avec l'Organe en charge de la certification racine dans le cadre de la qualification d'un service de confiance sont protégés en confidentialité au moyen d'outils définis conjointement entre l'Organe en charge de la certification racine et le commanditaire.

Article 401 Réclamations et recours

Le plaignant peut constituer une réclamation contre un service de confiance qualifié ou son prestataire, qu'il transmet à l'Organe en charge de la certification racine selon les modalités fixées par ce dernier.

Le commanditaire peut former un recours gracieux ou contentieux contre toute décision de refus de la demande de qualification, et contre toute décision de refus ou de retrait de la qualification, dans un délai de trois (3) mois à compter de la décision objet du recours.

Le commanditaire forme son recours gracieux auprès de l'Organe en charge de la certification racine selon les modalités prévues par ce dernier. L'Organe en charge de la certification racine accuse réception auprès du commanditaire, par voie postale ou électronique, du recours puis désigne un chargé de qualification en charge de l'instruction du recours.

Dans le cadre de l'instruction du recours, le chargé de qualification peut inviter le commanditaire à motiver son recours au cours d'une ou plusieurs réunions. Le recours n'est pas suspensif de la décision de qualification.

Le commanditaire forme son recours contentieux auprès des juridictions compétentes.

Article 402 Interruption

Le processus de qualification peut être interrompu dans l'un des cas suivants :

1. le commanditaire ne respecte pas un engagement pris dans le dossier de demande de qualification ;

2. le commanditaire ne respecte pas le délai fixé par l'Organe en charge de la certification racine pour franchir un jalon du processus de qualification ;

3. un jalon du processus de qualification ne peut être franchi pour des raisons détaillées dans la décision d'interruption de l'Organe en charge de la certification racine.

La décision d'interruption du processus de qualification peut être prononcée de manière unilatérale par l'Organe en charge de la certification racine ou par le commanditaire et à tout moment après la décision d'acceptation de la demande de qualification.

Lorsque la décision d'interruption du processus de qualification est prononcée avant la décision d'octroi de la qualification, l'Organe en charge de la certification racine prend une décision de refus de qualification conformément aux dispositions de l'Article 394. Lorsque la décision d'interruption du processus de qualification est prononcée après la décision d'octroi de la qualification, l'Organe en charge de la certification racine peut prendre une décision de maintien de la qualification avec modification ou une décision de retrait de la qualification.

Article 403 Notification de l'interruption

Lorsque la décision d'interruption du processus de qualification est prise par le commanditaire, ce dernier en informe l'Organe en charge de la certification racine, selon les modalités prévues par ce dernier, en y précisant les motifs.

Lorsque la décision d'interruption du processus de qualification est prise par l'Organe en charge de la certification racine, ce dernier en informe le commanditaire, selon les modalités prévues par lui.

En cas d'interruption du processus de qualification, le commanditaire peut soumettre, à une date ultérieure, une nouvelle demande de qualification pour le même service de confiance. Il ne peut en revanche pas, dans ce cas, se prévaloir des jalons franchis lors de l'instruction précédemment interrompue.

Article 404 Suivi de la qualification

Un suivi de la qualification ayant pour objectif de s'assurer, après toute décision d'octroi de la qualification, que les critères sur la base desquels la qualification a été octroyée sont toujours respectés sera conduit par l'Organe en charge de la certification racine.

Article 405 Certificats qualifiés délivrés par des prestataires de services de confiance étrangers

Les certificats qualifiés délivrés au public par des prestataires de services de confiance étrangers ont la même valeur et sont assimilés aux certificats délivrés par un prestataire de services de confiance établi en République de Djibouti si :

1. le prestataire de services de confiance étranger remplit les conditions du présent Code, après vérification par les autorités compétentes ; ou

2. le certificat ou le prestataire de services de confiance est reconnu en application d'un accord, traité ou tout autre texte national ou international pertinent conclu entre la République de Djibouti et un ou plusieurs pays ou organisations internationales.

Section 2 : Obligations et responsabilité des prestataires de services de confiance

Article 406 Protection des données à caractère personnel

Sans préjudice des dispositions du Livre Premier, les prestataires de services de confiance qualifiés et non qualifiés qui délivrent des certificats au public ne peuvent recueillir des données personnelles que directement auprès de la personne concernée, avec le consentement explicite de celle-ci, et uniquement dans la mesure où cela est nécessaire à la délivrance et à la conservation du certificat.

Les données qui leurs sont transmises, en particulier les données à caractère personnel, ne peuvent être recueillies ni traitées à d'autres fins sans le consentement explicite préalable de la personne concernée. Les prestataires ne peuvent détenir, consulter et exploiter ces données que dans la mesure strictement nécessaire à l'accomplissement de leurs services.

Lorsque le titulaire du certificat utilise un pseudonyme et lorsque les nécessités d'enquêtes de police ou d'enquêtes judiciaires l'exigent, le prestataire de services de confiance ayant délivré le certificat est tenu de communiquer à l'Organe en charge de la certification racine, à la police ou à l'autorité judiciaire toute donnée et/ou information relative à l'identité du titulaire.

Article 407 Obligations en matière de sécurité

Les prestataires de services de confiance qualifiés et non qualifiés prennent les mesures techniques et organisationnelles nécessaires, afin de prévenir et gérer les risques liés à la sécurité des services de confiance qu'ils fournissent.

Compte tenu des évolutions technologiques les plus récentes, ces mesures garantissent que le niveau de sécurité soit proportionné au degré de risques.

Des mesures sont notamment prises en vue de prévenir et limiter les conséquences d'incidents liés à la sécurité et d'informer les parties concernées des effets préjudiciables de tels incidents.

Article 408 Obligation de notification des incidents de sécurité

Les prestataires de services de confiance qualifiés et non qualifiés notifient à l'Organe en charge de la certification racine, dans les meilleurs délais et au plus tard dans un délai de vingt-quatre (24) heures après en avoir eu connaissance, toute atteinte à la sécurité ou toute perte d'intégrité ayant une incidence significative sur le service de confiance fourni ou sur les données à caractère personnel qui y sont conservées.

Article 409 Exigences applicables aux prestataires de services de confiance qualifiés

Lorsqu'un prestataire de services de confiance qualifié délivre un certificat qualifié pour un service de confiance, il vérifie par des moyens appropriés l'identité et, le cas échéant, tous les attributs spécifiques de la personne physique ou morale à laquelle il délivre le certificat qualifié.

Ces informations sont vérifiées par le prestataire de services de confiance qualifié ou par un tiers, notamment :

1. par la présence physique de la personne physique concernée ou du représentant autorisé de la personne morale ;

2. au moyen d'un certificat de signature électronique qualifié ou de cachet électronique qualifié ; ou

3. à l'aide d'autres méthodes d'identification reconnues en République de Djibouti, qui fournissent une garantie équivalente, en termes de fiabilité, à la présence physique de la personne physique concernée ou du représentant autorisé de la personne morale. La garantie équivalente est confirmée par un organisme d'évaluation de la conformité.

Un prestataire de services de confiance qualifié doit :

1. informer l'Organe en charge de la certification racine de toute modification dans la fourniture de ses services de confiance qualifiés et de son intention éventuelle de cesser ses activités ;

2. démontrer qu'il dispose des moyens techniques fiables en vue de fournir les services de confiance qualifiés en toute sécurité ;

3. assurer le fonctionnement de services d'annuaire et de révocation sûrs et rapides ;

4. veiller à ce que la date et l'heure d'émission et de révocation d'un certificat puissent être déterminées avec précision ;

5. prendre des mesures contre la contrefaçon des certificats et, dans les cas où le prestataire de services de confiance génère des données afférentes à la création de signature ou de cachet électronique, garantir la confidentialité au cours du processus de génération de ces données ;

6. disposer des ressources financières suffisantes pour mener convenablement son activité ;

7. souscrire une police d'assurance garantissant les dommages susceptibles d'être causés dans l'exercice de cette activité ;

8. employer du personnel et sous-traitants disposant de l'expertise, de l'expérience et des qualifications nécessaires en matière de sécurité des réseaux et systèmes d'informations et de protection des données à caractère personnel, et appliquant des procédures administratives et de gestion correspondant aux normes nationales et internationales ;

9. informer les utilisateurs de services de confiance qualifiés, de manière claire, exhaustive et avant toute relation contractuelle, sur les conditions précises d'utilisation du service, y compris les limites à son utilisation, les procédures de réclamation et de règlement des litiges. Cette information peut être transmise par voie électronique, doit faire l'objet d'un écrit et doit être aisément compréhensible. Des éléments pertinents de cette information doivent également, sur demande, être mis à la disposition des tiers qui se prévalent du certificat ;

10. utiliser des systèmes et équipements fiables, protégés contre les risques de modifications et assurant la sécurité technique des processus pris en charge ;

11. utiliser des systèmes fiables de stockage des données qui lui sont communiquées, sous une forme vérifiable de sorte que :

    a. les données ne soient publiquement disponibles pour des traitements qu'après avoir obtenu le consentement de la personne concernée ;

    b. seules des personnes autorisées puissent introduire des données et modifier les données conservées ;

    c. l'authenticité des données puisse être vérifiée ;

12. prendre les mesures appropriées contre la falsification et le vol de données ;

13. enregistrer, conserver et maintenir accessibles pour une durée appropriée, y compris après la cessation des activités du prestataire de services de confiance qualifié, toutes les informations pertinentes concernant les données envoyées et reçues par le prestataire de services de confiance qualifié, notamment à des fins probatoires et de continuité du service ;

14. disposer d'un plan actualisé d'arrêt d'activité afin d'assurer la continuité du service ;

15. assurer le traitement licite des données à caractère personnel conformément aux dispositions du Livre Premier ;

16. le cas échéant, établir et tenir à jour une base de données des certificats octroyés ;

17. s'assurer que les certificats ne sont disponibles au public que dans les cas où le titulaire du certificat a donné son consentement ;

18. s'assurer que toute modification technique mettant en péril les exigences de sécurité soit apparente.

Les prestataires de services de confiance qualifiés fournissent aux utilisateurs les informations pertinentes sur la validité ou le statut de révocation des certificats qualifiés qu'ils ont délivrés. Ces informations sont disponibles pour chaque certificat, à tout moment et durant la période de validité du certificat, sous une forme lisible, fiable et gratuite.

Section 3 : Responsabilité des prestataires de services de confiance et charge de la preuve

Article 410 Responsabilité des prestataires de services de confiance

Sans préjudice des dispositions de l'alinéa 2, les prestataires de services de confiance qualifiés et non qualifiés sont responsables des dommages causés intentionnellement, par négligence ou par maladresse à toute personne physique ou morale en raison d'un manquement aux obligations prévues aux dispositions du présent Code.

Lorsque les prestataires de services de confiance qualifiés et non qualifiés informent préalablement leurs utilisateurs des limites qui existent à l'utilisation des services qu'ils fournissent et que ces limites peuvent être reconnues par des tiers, ils ne peuvent être tenus responsables des dommages découlant de l'utilisation desdits services au-delà des limites ainsi définies.

Article 411 Charge de la preuve

Il incombe à la personne physique ou morale qui invoque les dommages visés à l'Article 410, d'apporter la preuve que le prestataire de services de confiance non-qualifié a agi intentionnellement, par maladresse ou par négligence.

Un prestataire de services de confiance qualifié est présumé responsable, à moins qu'il n'apporte la preuve que les dommages visés à l'Article 410 aient été causés sans intention, maladresse ou négligence de sa part.

Section 4 : Titulaires de certificats et révocation des certificats qualifiés

Article 412 Obligations des titulaires de certificats

En cas de doute ou de risque de violation de la confidentialité des données relatives à la signature ou au cachet électronique, ou en cas de défaut de conformité par rapport aux informations contenues dans le certificat, le titulaire est tenu de faire révoquer le certificat.

Lorsqu'un certificat est arrivé à échéance ou a été révoqué, le titulaire ne peut, après l'expiration du certificat ou après sa révocation, utiliser les données relatives à la signature pour signer ou faire certifier ces données par un autre prestataire de services de confiance.

Article 413 Responsabilité des titulaires de certificats

Dès la création des données relatives à la signature ou au cachet électronique, le titulaire du certificat devient responsable de la confidentialité de ces données.

Article 414 Révocation des certificats

A la demande du titulaire du certificat préalablement identifié, le prestataire de services de confiance qualifié révoque immédiatement le certificat.

Le prestataire de services de confiance qualifié doit enregistrer cette révocation dans sa base de données de certificats. Le statut de révocation du certificat est publié dans la liste visée à l'Article 399 dans les vingt-quatre (24) heures suivant la réception de la demande.

Le prestataire de services de confiance qualifié révoque également un certificat lorsque :

1. le prestataire de services de confiance qualifié cesse ses activités sans qu'il n'y ait reprise de celles-ci par un autre prestataire de services de confiance garantissant un niveau de qualité et de sécurité équivalent ;

2. il existe des raisons sérieuses de penser que le certificat a été délivré sur la base d'informations erronées ou falsifiées, que les informations contenues dans le certificat ne sont plus valides ou que la confidentialité des données afférentes à la signature ait été violée ou risque de l'être ;

3. le prestataire de services de confiance est informé du décès de la personne physique ou de la dissolution de la personne morale qui en est titulaire.

Sauf en cas de décès, le prestataire de services de confiance qualifié notifie la révocation du certificat au titulaire, dans un délai d'un (1) mois avant la révocation du certificat. La décision de révocation doit être motivée. La révocation est enregistrée dans la base de données de certificats tenue par le prestataire de services de confiance qualifié, et publiée dans la liste visée à l'Article 399.

La révocation d'un certificat est effective, définitive et opposable aux tiers à compter de la date de sa publication.

Section 5 : Autorité de certification racine

Article 415 Organe en charge de la certification racine

L'Organe en charge de la certification racine constitue l'autorité de certification racine en République de Djibouti.

Article 416 Missions de l'Organe en charge de la certification racine

L'Organe en charge de la certification racine est chargé des missions suivantes :

1. Définit les modalités de fourniture des services de certification électronique sur le territoire de la République de Djibouti ;
2. Octroie les autorisations d'exercice de l'activité de fournisseur de services de certification électronique sur le territoire de la République de Djibouti ;
3. Contrôle le respect par les fournisseurs de services de certification électronique des dispositions de la présente loi et de ses textes d'applications ;
4. Conclut les conventions de reconnaissance mutuelle des services de certification électronique avec les autorités étrangères ;
5. Emet, délivre et conserve les certificats électroniques relatifs aux agents publics habilités à effectuer des échanges électroniques, étant entendu que ces opérations peuvent être effectuées directement ou à travers des fournisseurs de services de certification électronique ;
6. Participe à la sécurisation des transactions et des échanges électroniques, notamment en participant aux activités de recherche, de formation et d'étude ;
7. Participe à toute activité qui lui a été confiée par le Ministère chargé de l'économie numérique en rapport avec son champ d'intervention ;
8. Toutes questions relatives au développement des moyens ou prestations de cryptologie de nature civile ;

Les dispositions du présent article peuvent être précisées par décret en Conseil des ministres sur proposition du ministère en charge de l'économie numérique

Article 417 Exercice des missions de l'Organe en charge de la certification racine

En l'absence de création d'une entité distincte, le Ministère en charge de l'économie numérique assure les missions de l'Organe en charge de la certification racine.

Chapitre 2 : Contrôle des prestataires de services de confiance

Article 418 Autorité de contrôle des services de confiance

L'autorité de contrôle des services de confiance qualifiés et non qualifiés en République de Djibouti est l'Organe en charge de la certification racine.

Article 419 Prérogatives de l'autorité de contrôle des services de confiance

Dans le cadre de ses prérogatives de contrôle, l'Organe en charge de la certification racine a notamment la possibilité de :

1. accorder le statut « qualifié » aux prestataires de services de confiance et aux services qu'ils fournissent et retirer ce statut conformément aux dispositions du présent Code ;

2. informer les autorités compétentes de ses décisions d'accorder ou de retirer le statut «qualifié»;

3. analyser les rapports d'évaluation de conformité des prestataires de services de confiance qualifiés ;

4. procéder, notamment via un organisme d'évaluation de conformité, à des audits et des évaluations de conformité des prestataires de services de confiance qualifiés ;

5. informer, le cas échéant, les autres organes de contrôle et le public de toute atteinte à la sécurité ou perte d'intégrité ;

6. exiger que les prestataires de services de confiance corrigent tout manquement aux obligations prévues au présent Code ;

7. vérifier l'existence et la bonne application des dispositions relatives aux plans d'arrêt d'activité lorsque le prestataire de services de confiance qualifié cesse ses activités, y compris la façon dont les informations restent accessibles.

Article 420 Audit périodique des prestataires de services de confiance

Tous les douze (12) mois les prestataires de services de confiance qualifiés transmettent un rapport d'évaluation de conformité de leurs activités au présent Code à l'Organe en charge de la certification racine.

Les prestataires de services de confiance qualifiés font l'objet, au moins tous les vingt-quatre (24) mois, d'un audit effectué à leurs frais par un organisme d'évaluation de la conformité.

L'objet de cet audit est de confirmer que lesdits prestataires et les services qu'ils fournissent remplissent les exigences fixées par le présent livre.

Article 421 Audit et évaluation ponctuels des prestataires de services de confiance

Sans préjudice des dispositions de l'article précédent, l'Organe en charge de la certification racine peut à tout moment soumettre les prestataires de services de confiance qualifiés à un audit ou demander à un organisme d'évaluation de la conformité de procéder à une évaluation de la conformité des prestataires de services de confiance qualifiés, aux frais de ces derniers, afin de s'assurer que lesdits prestataires et les services qu'ils fournissent remplissent les exigences fixées par le présent livre.

Les contrôles ponctuels de conformité effectués par l'Organe en charge de la certification racine ne peuvent être abusifs et doivent être justifiés au regard de la situation du prestataire de services de confiance qualifié et des éléments le concernant dont elle dispose.

Article 422 Correction des manquements des prestataires de services de confiance

Lorsque l'Organe en charge de la certification racine exige du prestataire de services de confiance qualifié la correction d'un manquement aux exigences prévues par le présent Code et que le prestataire n'agit pas en conséquence, cette dernière a la possibilité, en tenant compte de l'ampleur, de la durée et des conséquences du manquement, de saisir la juridiction compétente, notamment afin de :

1. faire cesser la délivrance de certificats qualifiés par le prestataire de services de confiance ;

2. obliger le prestataire de services de confiance à informer immédiatement les titulaires des certificats qualifiés qu'il a délivrés, de leur non-conformité aux dispositions du présent Code.

Article 423 Retrait de la déclaration de prestataire de services de confiance

Lorsque l'Organe en charge de la certification racine exige du prestataire de services de confiance la correction d'un manquement aux exigences prévues par le présent Code et que le prestataire n'agit pas en conséquence, cette dernière a la possibilité, en tenant compte de l'ampleur, de la durée et des conséquences du manquement, de retirer la déclaration du prestataire de services de confiance concerné. Le cas échéant, l'Organe en charge de la certification racine informe le prestataire de services de confiance du retrait de sa déclaration.

Article 424 Retrait du statut qualifié du prestataire de services de confiance

Lorsque l'Organe en charge de la certification racine exige du prestataire de services de confiance qualifié la correction d'un manquement aux exigences prévues par le présent Code et que le prestataire n'agit pas en conséquence, cette dernière a la possibilité, en tenant compte de l'ampleur, de la durée et des conséquences du manquement, de retirer le statut qualifié du prestataire de services de confiance concerné.

Le cas échéant, l'Organe en charge de la certification racine met à jour la liste des prestataires de services de confiance qualifiés visée à l'Article 399 et informe le prestataire de services de confiance du retrait de son statut qualifié.

Article 425 Sanctions pénales et publication du jugement définitif

Est puni d'une peine de 3 à 5 mois d'emprisonnement et d'une amende de 350.000 DJF à 7.000.000 DJF ou de l'une de ces peines seulement, quiconque aura usurpé la qualité de prestataire de services de confiance.

Les peines prévues à l'alinéa premier sont portées au double en cas d'usurpation de la qualité de prestataire de services de confiance qualifié.

En condamnant du chef d'infraction visé au premier alinéa, la juridiction compétente peut ordonner l'insertion du jugement, intégralement ou par extraits, dans un ou plusieurs journaux, dans les conditions qu'elle détermine, aux frais de la personne condamnée.

Chapitre 3 : Signature électronique

Section 1 : Dispositions générales

Article 426 Effets juridiques de la signature électronique

L'effet juridique d'une signature électronique qualifiée est équivalent à celui d'une signature manuscrite.

L'effet juridique et la recevabilité d'une signature électronique comme preuve en justice ne peuvent être refusés au seul motif que cette signature se présente sous une forme électronique ou qu'elle ne satisfait pas aux exigences de la signature électronique qualifiée.

Article 427 Exigences applicables aux signatures électroniques avancées

Une signature électronique avancée satisfait aux exigences suivantes :

1. être liée au signataire de manière univoque ;

2. permettre d'identifier le signataire ;

3. avoir été créée à l'aide de données de création de signature électronique que le signataire peut, avec un niveau de confiance élevé fixé par l'Organe en charge de la certification racine, utiliser sous son contrôle exclusif ;

4. être liée aux données associées à cette signature de telle sorte que toute modification ultérieure des données soit détectable.

Ces exigences peuvent être complétées par décret pris en Conseil des ministres, sur proposition du Ministre chargé de l'économie numérique.

Article 428 Exigences applicables aux signatures électroniques qualifiées

Une signature électronique qualifiée satisfait aux exigences suivantes :

1. satisfaire aux exigences applicables aux signatures électroniques avancées ;

2. être créée au moyen d'un dispositif qualifié de création de signatures électroniques ;

3. avoir reçu un certificat qualifié de signature électronique délivré par un prestataire de services de confiance qualifié.

Ces exigences peuvent être complétées par décret pris en Conseil des ministres, sur proposition du Ministre chargé de l'économie numérique.

Section 2 : Création de signature électronique

Article 429 Exigences applicables aux dispositifs de création de signature électronique

Le dispositif de création de signature électronique doit permettre de :

1. conserver et utiliser la clé privée au moyen de tout procédé de sécurisation fiable;

2. cacher la clé privée après chaque utilisation.

Article 430 Exigences applicables aux dispositifs qualifiés de création de signature électronique

Les dispositifs qualifiés de création de signature électronique doivent répondre aux exigences suivantes :

1. garantir, par des moyens techniques et des procédures appropriées, que les données de création de signatures électroniques utilisées :

    a. sont confidentielles ;

    b. ne peuvent être établies qu'une seule fois ;

    c. ne peuvent être identifiées par déduction ;

    d. peuvent être protégées de manière fiable par le signataire contre toute utilisation de tiers.

2. protéger la signature électronique de manière fiable, par tout moyen technique disponible, contre toute falsification ;

3. ne pas modifier les données à signer et ne pas empêcher la présentation de ces données au signataire avant la signature.

Ces exigences peuvent être complétées par décret pris en Conseil des ministres, sur proposition du Ministre chargé de l'économie numérique.

Article 431 Certification des dispositifs qualifiés de création de signature électronique qualifiée

La conformité des dispositifs qualifiés de création de signature électronique avec les exigences fixées par l'Article 430 est certifiée par l'autorité visée à l'Article 415.

Cette certification est fondée sur l'un des éléments suivants :

1. un processus d'évaluation de la sécurité mis en œuvre par l'autorité visée à l'Article 415 ; ou

2. tout autre processus, à condition qu'il recourt à des niveaux de sécurité comparables. Ledit processus ne peut être utilisé qu'en l'absence du processus visé au point (1) ou lorsqu'un tel processus est en cours.

Article 432 Utilisation de la cryptographie asymétrique

La création de signature électronique doit utiliser un dispositif comprenant une paire de clés composée d'une clé privée et d'une clé publique, selon les principes de la cryptographie asymétrique.

Article 433 Clés de chiffrement

Les clés de chiffrement doivent, en tenant compte du progrès technique, être conformes :

1. aux normes en vigueur en la matière ;
2. aux conditions des algorithmes de création et de vérification de la signature définie au cahier des charges des prestataires de services de confiance qualifiés.

Article 434 Caractère personnel d'une paire de clés

Une paire de clé est unique, personnelle, non-cessible et non-transférable.

Article 435 Registre des clés publiques

La personne ayant émis la paire de clés transmet la clé publique à l'Organe en charge de la certification racine, qui tient à la disposition de tous un registre des clés publiques.

Section 3 : Certification de signature électronique

Article 436 Exigences applicables aux certificats qualifiés de signature électronique

Un certificat de signature électronique est qualifié lorsqu'il contient :

1. une mention expresse indiquant que le certificat délivré est un certificat qualifié de signature électronique ;
2. l'ensemble de données représentant sans ambiguïté le prestataire de services de confiance qualifié délivrant les certificats qualifiés ;
3. le nom du signataire ;
4. les données de validation de la signature électronique correspondant aux données de création de la signature électronique ;
5. les dates et/ou heures de début et de fin de validité du certificat ;
6. le code d'identification du certificat, qui doit être unique pour le prestataire de services de confiance qualifié ;

7. la signature électronique qualifiée du prestataire de services de confiance qualifié délivrant le certificat ;

8. l'endroit où peut être obtenu gratuitement le certificat sur lequel repose la signature électronique qualifiée du prestataire de services de confiance qualifié délivrant le certificat et contenant la clé publique complémentaire de la clé privée utilisée par ce prestataire de services pour signer ;

9. l'emplacement des services qui peuvent être utilisés pour connaître le statut de validité du certificat qualifié ;

10. une mention expresse indiquant si les données de création de la signature électronique associées aux données de validation de la signature électronique se trouvent dans un dispositif qualifié de création de signature électronique.

Les exigences suivantes peuvent être complétées par décret pris en Conseil des ministres, sur proposition du Ministre chargé de l'économie numérique.

Article 437 Vérifications opérées par le prestataire de services de confiance

Le prestataire de services de confiance vérifie que :

1. l'utilisateur éventuel détient une clé privée capable de créer une signature électronique ;

2. cette clé privée est complémentaire de la clé publique devant être signalée dans le certificat devant être émis ;

3. la clé publique indiquée dans le certificat de signature électronique est capable de vérifier une signature électronique à laquelle est apposée la clé publique.

Article 438 Délivrance des certificats de signature électronique

Le prestataire de services de confiance qualifié délivre les certificats de signature électronique après s'être conformé à la procédure de vérification, et après avoir remis à l'utilisateur les informations nécessaires à l'utilisation correcte et sûre de ses services, à savoir :

1. les conditions contractuelles de délivrance d'un certificat ;

2. les obligations pesant sur le titulaire du certificat et le prestataire de services de confiance qualifié ;

3. les modalités et les conditions précises d'utilisation des certificats, y compris les limites imposées à leur utilisation ;

4. les procédures de réclamation et de règlement des litiges.

Ces informations doivent être approuvées, au préalable, par l'Organe en charge de la certification racine.

Les certificats sont transmis à l'Organe en charge de la certification racine pour inscription sur le registre des clés publiques.

Article 439 Renouvellement d'un certificat de signature électronique

Un certificat de signature électronique est renouvelé sur demande de son titulaire, transmise par écrit à l'Organe en charge de la certification racine par le prestataire de services de confiance qualifié dans les deux (2) mois précédant la fin de la période de validité dudit certificat.

Article 440 Révocation du certificat de signature électronique

A la demande du titulaire du certificat de signature électronique préalablement identifié, le prestataire de services de confiance qualifié révoque immédiatement le certificat.

Le prestataire de services de confiance qualifié doit enregistrer cette révocation dans sa base de données de certificats. Le statut de révocation du certificat est publié dans la liste visée à l'Article 399 dans les vingt-quatre (24) heures suivant la réception de la demande.

Le prestataire de services de confiance qualifié révoque également un certificat lorsque :

1. la validité du certificat expire et le titulaire du certificat ne donne pas suite à la notification d'approche d'expiration du prestataire de services de confiance qualifié ;

2. le certificat a été délivré sur la base d'informations erronées ou falsifiées ;

3. les informations contenues dans le certificat ne sont plus conformes à la réalité ;

4. la confidentialité des données à caractère personnel du certificat a été violée ;

5. le certificat a été utilisé frauduleusement ;

6. le titulaire décède ou la personne morale est dissoute.

Sauf en cas de décès, le prestataire de services de confiance qualifié notifie la révocation du certificat au titulaire, dans un délai d'un (1) mois avant la révocation du certificat. La décision de révocation doit être motivée et enregistrée dans la base de données de certificats tenue par le prestataire de services de confiance qualifié et publiée dans la liste visée à l'Article 399.

La révocation d'un certificat est effective, définitive et opposable aux tiers à compter de la date de sa publication.

Article 441 Certificats de signature électronique délivrés par des prestataires de services de confiance étrangers

Un certificat de signature électronique qualifié hors du territoire national, en vertu du droit du lieu où il a été émis, produit en République de Djibouti les mêmes effets juridiques qu'un certificat de signature électronique qualifié conformément aux dispositions du présent titre, sous réserve que ce droit ne présente pas de garanties inférieures à celles prévues dans le Livre Quatrième.

Section 4 : Validation de la signature électronique

Article 442 Exigences relatives à la validation des signatures électroniques qualifiées

Le processus de validation d'une signature électronique qualifiée confirme la validité d'une signature électronique qualifiée, à condition que :

1. le certificat sur lequel repose la signature ait été, au moment de la signature, un certificat qualifié de signature électronique conforme aux exigences prévues par le Livre Quatrième ;

2. le certificat qualifié ait été délivré par un prestataire de services de confiance qualifié et était valide au moment de la signature ;

3. les données de validation de la signature correspondent aux données communiquées à la personne concernée ;

4. l'ensemble unique de données représentant le signataire dans le certificat soit correctement fourni à la personne concernée ;

5. l'utilisation d'un pseudonyme soit clairement indiquée, si un pseudonyme a été utilisé au moment de la signature ;

6. la signature électronique ait été créée par un dispositif de création de signature électronique qualifié ;

7. l'intégrité des données signées n'ait pas été compromise ;

8. la signature électronique respecte l'ensemble des exigences prévues au présent titre.

Le système utilisé pour valider la signature électronique qualifiée fournit à l'utilisateur le résultat exact du processus de validation et permet à celui-ci de détecter tout problème de sécurité.

Article 443 Services de validation qualifiés des signatures électroniques qualifiées

Un service de validation qualifié des signatures électroniques qualifiées ne peut être fourni que par un prestataire de services de confiance qualifié qui :

1. fournit une validation conformément aux exigences légales et réglementaires applicables à la validation des signatures électroniques qualifiées ;

2. permet aux utilisateurs de recevoir le résultat du processus de validation d'une manière automatisée, fiable, efficace et portant la signature électronique avancée ou le cachet électronique avancé du prestataire qui fournit le service de validation qualifié.

Section 5 : Conservation de signature électronique

Article 444 Exigences relatives aux services de conservation qualifiés des signatures électroniques

Un service de conservation qualifié des signatures électroniques ne peut être fourni que par un prestataire de services de confiance qualifié qui utilise des procédures et des technologies permettant d'étendre la fiabilité des signatures électroniques qualifiées au-delà de la période de validité technologique.

Chapitre 4 : Cachet électronique

Article 445 Effets juridiques du cachet électronique

L'effet juridique et la recevabilité d'un cachet électronique ne peuvent être refusés au seul motif que ce cachet se présente sous forme électronique ou qu'il ne satisfait pas aux exigences du cachet électronique qualifié.

Un cachet électronique qualifié bénéficie d'une présomption d'intégrité des données et d'exactitude de l'origine des données auxquelles il est lié. Le cachet électronique qualifié a un effet juridique équivalent à un cachet manuscrit.

Article 446 Utilisation de cachets électroniques dans les services publics

Lorsqu'un cachet électronique est exigé pour utiliser un service public en ligne, sont reconnus les cachets électroniques avancés et les cachets électroniques qualifiés.

L'utilisation des cachets électroniques dans le secteur public peut être soumise à des exigences supplémentaires, fixées par décret pris en Conseil des ministres, sur proposition du Ministre chargé de l'économie numérique. Ces exigences doivent être objectives, transparentes, proportionnées et non-discriminatoires.

Article 447 Exigences applicables aux cachets électroniques avancés

Un cachet électronique avancé satisfait aux exigences suivantes :

1. être lié au créateur du cachet de manière univoque ;

2. permettre d'identifier le créateur du cachet ;

3. avoir été créé à l'aide de données de création de cachet électronique que le créateur du cachet peut, avec un niveau de confiance élevé, utiliser sous son contrôle pour créer un cachet électronique ;

4. être lié aux données auxquelles il est associé de sorte que toute modification ultérieure des données soit détectable.

Ces exigences peuvent être complétées par décret pris en Conseil des ministres, sur proposition du Ministère en charge de l'économie numérique.

Article 448 Exigences applicables aux cachets électroniques qualifiés

Un cachet électronique qualifié satisfait aux exigences suivantes :

1. satisfaire aux exigences applicables aux cachets électroniques avancés ;

2. être créé à l'aide d'un dispositif de création de cachet électronique qualifié ;

3. reposer sur un certificat qualifié de cachet électronique.

Ces exigences peuvent être complétées par décret pris en Conseil des ministres, sur proposition du Ministre chargé de l'économie numérique.

Article 449 Certificats qualifiés de cachet électronique

Les certificats qualifiés de cachet électronique doivent satisfaire aux exigences fixées par décret pris en Conseil des ministres, sur proposition du Ministère chargé de l'économie numérique. Ils ne font l'objet d'aucune exigence obligatoire allant au-delà des exigences ainsi fixées.

Article 450 Délivrance des certificats

Le prestataire de services de confiance délivre les certificats de cachet électronique après :

1. S'être conformé à la procédure de vérification correspondante au type de cachet électronique, qualifiée ou non qualifiée ;

2. Avoir remis à l'utilisateur les informations nécessaires à l'utilisation conforme et sécurisée de ses services de confiance, qui doivent être approuvées au préalable par l'Organe en charge de la certification racine. Les informations contiennent à minima :
   - Les conditions contractuelles de délivrance d'un certificat ;
   - Les obligations pesant sur le prestataire de services de confiance et sur le titulaire du certificat ;
   - Les modalités et les conditions précises d'utilisation des certificats ;
   - Les procédures de réclamation et de règlement des litiges.

Les certificats sont ensuite transmis à l'Organe en charge de la certification racine pour inscription sur le registre des clés publiques.

Article 451 Renouvellement des certificats

Le renouvellement du certificat de cachet électronique s'effectue sur demande de son titulaire adressée à l'Organe en charge de la certification racine par le prestataire de services de confiance dans les trois (3) mois précédant la fin de validité du certificat.

Article 452 Révocation des certificats qualifiés de cachet électronique

A la demande du titulaire du certificat qualifié de cachet électronique préalablement identifié, le prestataire de services de confiance qualifié révoque immédiatement le certificat.

Le prestataire de services de confiance qualifié doit enregistrer cette révocation dans sa base de données de certificats. Le statut de révocation du certificat est publié dans la liste visée à l'Article 399 dans les vingt-quatre (24) heures suivant la réception de la demande.

Le prestataire de services de confiance qualifié révoque également un certificat lorsque :

1. le prestataire de services de confiance qualifié cesse ses activités sans qu'il n'y ait reprise de celles-ci par un autre prestataire de services de confiance garantissant un niveau de qualité et de sécurité équivalent ;
2. il existe des raisons sérieuses de penser que le certificat a été délivré sur la base d'informations erronées ou falsifiées, que les informations contenues dans le certificat ne sont plus valides, que la confidentialité des données afférentes au cachet électronique ait été violée ou risque de l'être ou que le certificat qualifié a été utilisé frauduleusement ;

3. le prestataire de services de confiance est informé du décès de la personne physique ou de la dissolution de la personne morale qui en est titulaire.

Sauf en cas de décès, le prestataire de services de confiance qualifié notifie la révocation du certificat au titulaire, dans un délai d'un (1) mois avant la révocation du certificat. La décision de révocation doit être motivée et enregistrée dans la base de données de certificats tenue par le prestataire de services de confiance qualifié et publiée dans la liste visée à l'Article 399.

La révocation d'un certificat est effective, définitive et opposable aux tiers à compter de la date de sa publication.

Article 453 Dispositifs de création de cachets électroniques qualifiés

Les dispositifs de création de cachets électroniques qualifiés respectent les exigences définies par décret pris en Conseil des ministres, sur proposition du Ministre chargé de l'économie numérique. Cette certification est fondée sur l'un des éléments suivants :

- un processus d'évaluation de la sécurité mis en œuvre par l'Organe en charge de la certification racine ; ou

- tout autre processus, à condition qu'il recourt à des niveaux de sécurité comparables. Ce processus ne peut être utilisé qu'en l'absence d'un processus d'évaluation de la sécurité mis en œuvre par l'Organe en charge de la certification racine, ou lorsqu'un tel processus est en cours.

Article 454 Validation et conservation des cachets électroniques qualifiés

Le processus de validation d'un cachet électronique qualifié confirme la validité de ce dernier, à condition que :

1. le certificat sur lequel repose le cachet ait été, au moment du cachet, un certificat qualifié de cachet électronique conforme aux exigences prévues par voie réglementaire ;

2. le certificat qualifié ait été délivré par un prestataire de services de confiance qualifié et était valide au moment du cachet ;

3. les données de validation du cachet correspondent aux données communiquées à la personne concernée ;

4. l'ensemble unique des données dans le certificat soit correctement fourni à la personne concernée ;

5. l'utilisation d'un pseudonyme soit clairement indiquée, si un pseudonyme a été utilisé au moment du cachet ;

6. le cachet électronique ait été créé par un dispositif de création de cachet électronique qualifié ;

7. l'intégrité des données n'ait pas été compromise ;

8. le cachet électronique respecte l'ensemble des exigences prévues au présent Titre.

Le système utilisé pour valider le cachet électronique qualifié fournit à l'utilisateur le résultat exact du processus de validation et permet à celui-ci de détecter tout problème de sécurité.

Un service de validation des cachets électroniques qualifiés ne peut être fourni que par un prestataire de services de confiance qualifié qui :

1. fournit une validation conformément aux exigences légales et réglementaires applicables à la validation des cachets électroniques qualifiés ; et

2. permet aux utilisateurs de recevoir le résultat du processus de validation d'une manière automatisée, fiable, efficace et portant la signature électronique avancée ou le cachet électronique avancé du prestataire qui fournit le service de validation.

Article 455 Exigences relatives aux services de conservation qualifiés des cachets électroniques qualifiés

Un service de conservation qualifié des cachets électroniques qualifiés ne peut être fourni que par un prestataire de services de confiance qualifié qui utilise des procédures et des technologies permettant d'étendre la fiabilité des cachets électroniques qualifiés au-delà de la période de validité technologique.

Chapitre 5 : Identification électronique

Article 456 Utilisation de l'identification électronique

L'identification électronique est obligatoire pour toutes les institutions publiques, afin d'identifier les administrés et de faciliter la circulation des données et les services publics et parapublics.

Chapitre 6 : Horodatage électronique

Article 457 Effet juridique de l'horodatage électronique

L'effet juridique et la recevabilité d'un horodatage électronique ne peuvent être refusés comme preuve au seul motif que l'horodatage se présente sous forme électronique ou qu'il ne satisfait pas aux exigences de l'horodatage électronique qualifié.

Un horodatage électronique qualifié bénéficie d'une présomption d'exactitude de la date et de l'heure qu'il indique et d'intégrité des données auxquelles se rapportent ces dates et heures. L'horodatage électronique qualifié a un effet juridique équivalent à un horodatage manuscrit.

Article 458 Exigences applicables aux horodatages électroniques qualifiés

Tout horodatage électronique qualifié doit satisfaire aux exigences suivantes :

1. lier la date et l'heure aux données de manière à exclure la possibilité d'une modification indétectable de ces données ;

2. être fondé sur une horloge exacte liée au temps universel coordonné ; et

3. être signé au moyen d'une signature électronique avancée ou cacheté au moyen d'un cachet électronique avancé du prestataire de services de confiance qualifié, ou par une méthode équivalente.

Ces exigences peuvent être complétées par décret pris en Conseil des ministres, sur proposition du Ministère chargé de l'économie numérique.

Chapitre 7 : Archivage électronique et coffre-fort numérique

Article 459 Règles générales sur l'archivage électronique

L'archivage électronique consiste à mettre en place des actions, outils et méthodes afin de conserver des données, documents et informations en vue d'une utilisation ultérieure.

Les données concernées doivent être structurées, indexées et conservées sur des formats appropriés à la conservation et à la migration.

L'archivage doit garantir dans leur intégrité, la restitution des données conservées ou leur accessibilité dans un contexte technologique changeant.

Les règles de l'archivage électronique s'appliquent indifféremment aux documents numérisés et aux documents conçus initialement sur support électronique.

Article 460 Exigences applicables à l'archivage électronique

La conservation de documents électroniques archivés satisfait aux exigences suivantes :

1. l'information que contient le document est accessible et consultable ultérieurement ;

2. le document est conservé sous la forme sous laquelle il a été créé, envoyé ou reçu, ou sous une forme dont on peut démontrer qu'elle n'est susceptible ni de

modification, ni d'altération de son contenu, et que le document transmis et celui conservé sont strictement identiques ;

3. les informations qui permettent de déterminer l'origine et la destination du document, ainsi que les indications de date et d'heure de l'envoi ou de la réception doivent, le cas échéant, être conservées.

Ces exigences peuvent être complétées par décret pris en Conseil des ministres, sur proposition du Ministère chargé de l'économie numérique.

Article 461 Définition du service de coffre-fort numérique

Un service de coffre-fort numérique est un service qui a pour objet :

1. la réception, le stockage, la suppression et la transmission de données ou documents électroniques dans des conditions permettant de justifier de leur intégrité et de l'exactitude de leur origine ;

2. la traçabilité des opérations réalisées sur ces documents ou données et la disponibilité de cette traçabilité pour l'utilisateur ;

3. l'identification de l'utilisateur lors de l'accès au service par un moyen d'identification électronique ;

4. de garantir l'accès exclusif aux documents électroniques, données de l'utilisateur ou données associées au fonctionnement du service à cet utilisateur, aux tiers autres que le prestataire de service de coffre-fort numérique, explicitement autorisés par l'utilisateur à accéder à ces documents et données et, le cas échéant, au prestataire de service de coffre-fort numérique réalisant un traitement de ces documents ou données au seul bénéfice de l'utilisateur et après avoir recueilli son consentement ;

5. de donner la possibilité à l'utilisateur de récupérer les documents et les données stockées dans un standard ouvert aisément réutilisable et exploitable par un système de traitement automatisé de données, sauf dans le cas des documents initialement déposés dans un format non ouvert ou non aisément réutilisable qui peuvent être restitués dans leur format d'origine, dans des conditions définies par décret pris en Conseil des ministres, sur proposition du Ministre chargé de l'économie numérique.

Article 462 Obligation d'information sur les modalités de fonctionnement et d'utilisation du service de coffre-fort numérique

Le fournisseur d'un service de coffre-fort numérique est tenu à une obligation d'information claire, loyale et transparente sur les modalités de fonctionnement et d'utilisation du service, préalable à la conclusion d'un contrat.

Avant que l'utilisateur ne soit lié par un contrat de fourniture de service de coffre-fort numérique, le fournisseur du service lui communique, de manière lisible et compréhensible, les informations suivantes:

1. le type d'espace mis à sa disposition et les conditions d'utilisation associées ;
2. les mécanismes techniques utilisés ;
3. la politique de confidentialité ;
4. l'existence et les modalités de mise en œuvre des garanties de bon fonctionnement.

Ces informations sont également mises à disposition en ligne et, le cas échéant, mises à jour.

Article 463 Exigences applicables à la conservation de données dans un coffre-fort numérique

L'intégrité, la disponibilité et l'exactitude de l'origine des données et documents stockés dans le coffre-fort numérique sont garanties par des mesures de sécurité adaptées et conformes aux exigences précisées par décret pris en Conseil des ministres sur proposition du Ministre chargé de l'économie numérique.

Article 464 Traçabilité des opérations sur les données stockées dans le coffre-fort numérique

La traçabilité des opérations réalisées sur les données et documents stockés dans le coffre-fort numérique et la disponibilité de cette traçabilité pour l'utilisateur requièrent au minimum la mise en œuvre des mesures suivantes :

1. l'enregistrement et l'horodatage des accès et tentatives d'accès ;
2. l'enregistrement des opérations affectant le contenu ou l'organisation des données et documents de l'utilisateur ;
3. l'enregistrement des opérations de maintenance affectant les données et documents stockés dans le coffre-fort numérique.

Les durées de conservation de ces données de traçabilité constituent une mention obligatoire du contrat de fourniture de service de coffre-fort électronique.

Article 465 Modalités d'identification et d'accès au coffre-fort numérique

L'identification de l'utilisateur lors de l'accès au service de coffre-fort numérique est assurée par un moyen d'identification électronique adapté aux enjeux de sécurité du service.

Article 466 Récupération des données stockées dans le coffre-fort numérique

Avant que l'utilisateur ne conclue un contrat de fourniture de service de coffre-fort numérique, le fournisseur du service lui communique, de manière lisible et compréhensible, les modalités de l'opération de récupération de documents ou de données. A cette fin, il précise les informations suivantes :

1. les opérations techniques que l'utilisateur doit conduire pour la récupération des documents et données, les caractéristiques techniques du format du fichier de récupération ainsi que le délai de récupération ;

2. les conditions dans lesquelles le fournisseur du service de coffre-fort numérique peut être amené à procéder à une transformation du format dans lequel les documents et données ont été déposés ;

3. les frais éventuels exigibles.

Dans le cadre du processus de souscription, il recueille le consentement explicite de l'utilisateur à ces conditions, lesquelles sont mises en ligne de façon aisément accessible.

Pendant toute la durée du contrat de service de fourniture du coffre-fort numérique, l'utilisateur peut exercer à tout moment et à titre gratuit son droit à la récupération des documents et données, sans restriction sur le nombre d'opérations de récupération. Lorsque les demandes de récupération de l'utilisateur sont manifestement excessives, notamment en raison de leur caractère abusivement répétitif, le fournisseur du service de coffre-fort numérique peut :

1. exiger le paiement de frais raisonnables qui tiennent compte des coûts supportés pour organiser la récupération des documents et données demandées ; ou

2. refuser de donner suite à ces demandes.

Les dispositifs permettant à l'utilisateur d'un service de coffre-fort numérique de récupérer les documents et les données qui y sont stockés offrent la possibilité d'exercer cette récupération :

1. par voie de communication électronique, et par une requête unique, de façon simple et sans manipulation complexe ou répétitive ;

2. dans un format électronique ouvert, structuré, couramment utilisé, aisément réutilisable et exploitable par un système de traitement automatisé de données, sauf dans le cas des documents initialement déposés dans un format non ouvert qui peuvent être restitués dans leur format d'origine.

Le fournisseur du service de coffre-fort numérique prend toutes les mesures nécessaires, notamment en termes de protocoles de communication et d'interfaces de

programmation, afin que l'opération de récupération s'effectue de façon complète, intègre et dans un délai raisonnable. Il veille à ce que la mise en œuvre de cette fonctionnalité de récupération s'opère sans collecte de sa part d'informations confidentielles ou de données à caractère personnel concernant l'utilisateur du service, autres que celles indispensables à la bonne exécution de l'opération de récupération.

Les dispositifs permettant à l'utilisateur d'un service de coffre-fort numérique de récupérer les documents et données qui y sont stockés assurent un niveau d'intégrité et de confidentialité des documents et données au moins équivalent à celui des fonctions permettant la réception, le stockage, la suppression et la transmission de données.

Le fournisseur du service de coffre-fort numérique doit informer l'utilisateur au moins trois mois à l'avance de la suspension ou de la fermeture du service afin de lui permettre de récupérer les documents et donnés stockés dans son coffre-fort numérique.

En l'absence d'information préalable sur une suspension ou une fermeture de service, ou lorsque, quelle qu'en soit la raison, l'utilisateur cesse durablement d'être en mesure d'accéder au service de coffre-fort numérique, les dispositifs de récupération des documents et données restent disponibles et utilisables pendant une durée minimale de douze mois à compter de la date à laquelle cette cessation d'accès au service est intervenue.

Chapitre 8 : Recommandé électronique

Article 467 Effet juridique d'un recommandé électronique

L'effet juridique et la recevabilité des données envoyées et reçues à l'aide d'un service d'envoi recommandé électronique ne peuvent être refusés au seul motif que ce service se présente sous une forme électronique ou qu'il ne satisfait pas aux exigences du service d'envoi recommandé électronique qualifié.

Les données envoyées et reçues au moyen d'un service d'envoi recommandé électronique qualifié bénéficient d'une présomption quant à l'intégrité des données, à l'envoi de ces données par l'expéditeur identifié et à leur réception par le destinataire identifié, et à l'exactitude de la date et de l'heure de l'envoi et de la réception indiquées par le service d'envoi recommandé électronique qualifié.

Le recommandé électronique qualifié a un effet juridique équivalent à un envoi recommandé manuscrit.

Article 468 Consentement au recommandé électronique

Dans le cas où le destinataire n'est pas un professionnel, celui-ci doit avoir exprimé à l'expéditeur son consentement à recevoir des envois recommandés électroniques.

Article 469 Impression du recommandé électronique

Le prestataire de service d'envoi recommandé électronique qualifié ou non qualifié peut proposer que le contenu de l'envoi soit imprimé sur papier puis acheminé au destinataire.

Article 470 Preuve de dépôt électronique

Le prestataire de service d'envoi recommandé électronique qualifié ou non qualifié délivre à l'expéditeur une preuve du dépôt électronique de l'envoi.

Cette preuve de dépôt comporte les informations suivantes :

1. le nom et le prénom ou la raison sociale du destinataire ainsi que son adresse électronique ;

2. un numéro d'identification unique de l'envoi attribué par le prestataire ;

3. la date et l'heure du dépôt électronique de l'envoi indiquées par un horodatage électronique qualifié ;

4. la signature électronique avancée ou le cachet électronique utilisé par le prestataire lors de l'envoi.

Article 471 Information du destinataire d'un recommandé électronique

Le prestataire de service d'envoi recommandé électronique qualifié ou non qualifié informe le destinataire, par voie électronique, qu'un recommandé électronique lui est destiné et qu'il a la possibilité, pendant un délai de quinze (15) jours à compter du lendemain de l'envoi de cette information, d'accepter ou non sa réception.

Le destinataire n'est pas informé de l'identité de l'expéditeur du recommandé électronique qualifié ou non qualifié.

Article 472 Modalités de remise d'un recommandé électronique

En cas d'acceptation par le destinataire du recommandé électronique, le prestataire de service d'envoi recommandé électronique qualifié ou non qualifié procède à sa transmission.

Outre les informations mentionnées dans la preuve de dépôt, la preuve de réception comporte la date et l'heure de réception de l'envoi, indiquées par un horodatage électronique qualifié.

En cas de refus de réception ou de non-réclamation par le destinataire, le prestataire met à disposition de l'expéditeur, au plus tard le lendemain de l'expiration du délai de quinze (15) jours, une preuve de ce refus ou de cette non-réclamation.

Outre les informations mentionnées dans la preuve de dépôt, la preuve de refus précise la date et l'heure du refus telles qu'indiquées par un horodatage électronique qualifié.

Article 473 Conservation des preuves de dépôt et de remise

Le prestataire de service d'envoi recommandé électronique qualifié ou non qualifié doit conserver les preuves de dépôt et de remise du recommandé électronique pour une durée qui ne peut être inférieure à un (1) an.

Le prestataire de service d'envoi recommandé électronique qualifié ou non qualifié doit conserver la preuve de refus ou de non-réclamation du destinataire pour une durée qui ne peut être inférieure à un (1) an.

Article 474 Exigences applicables aux services d'envoi recommandé électronique qualifiés

Les services d'envoi recommandé électronique qualifiés doivent satisfaire aux exigences suivantes :

1. ils sont fournis par un ou plusieurs prestataires de services de confiance qualifiés ;
2. ils garantissent l'identification de l'expéditeur avec un degré de confiance élevé ;
3. ils garantissent l'identification du destinataire avant la fourniture des données ;
4. l'envoi et la réception de données sont sécurisés par une signature électronique avancée ou par un cachet électronique avancé d'un prestataire de services de confiance qualifié, de manière à exclure toute possibilité de modification indétectable des données ;
5. toute modification des données nécessaire pour l'envoi ou la réception de celles-ci est clairement signalée à l'expéditeur et au destinataire des données ;
6. la date et l'heure d'envoi, de réception et toute modification des données sont indiquées par un horodatage électronique qualifié.

Ces exigences peuvent être complétées par décret pris en Conseil des ministres, sur proposition du Ministère chargé de l'économie numérique.

Dans le cas où les données sont transférées entre deux prestataires de services de confiance qualifiés ou plus, les exigences fixées aux points 1 à 6 s'appliquent à tous les prestataires de services de confiance qualifiés.

Chapitre 9 : Authentification de sites Internet

Article 475 Exigences applicables aux certificats qualifiés d'authentification de sites Internet

L'authentification d'un site internet est assurée à travers un certificat qualifié d'authentification dudit site. Un tel certificat permet de s'assurer de la véracité du site internet et de l'associer à la personne physique ou morale à laquelle le certificat est délivré. Il ne peut être délivré que par un prestataire de services de confiance qualifié.

Les certificats qualifiés d'authentification de sites internet doivent satisfaire aux exigences suivantes :

1. une mention indiquant au moins sous une forme adaptée au traitement automatisé, que le certificat a été délivré comme certificat qualifié d'authentification de sites Internet ;

2. un ensemble de données identifiant sans ambiguïté le prestataire de services de confiance qualifié qui a délivré les certificats qualifiés, comprenant au moins sa raison sociale et/ou sa dénomination sociale, ainsi que son adresse exacte ;

3. pour les personnes physiques, au moins le nom, le prénom et l'adresse de la personne à qui le certificat est délivré ;

4. pour les personnes morales, au moins la raison sociale, la dénomination sociale et l'adresse du siège de la personne morale à laquelle le certificat est délivré ;

5. le(s) nom(s) de domaine exploité(s) par la personne physique ou morale à laquelle le certificat est délivré ;

6. toute information utile sur le début et la fin de la période de validité du certificat ;

7. le code d'identité du certificat, qui est unique pour le prestataire de services de confiance qualifié ;

8. la signature électronique avancée ou le cachet électronique avancé du prestataire de services de confiance qualifié délivrant le certificat, ainsi que l'adresse où ils peuvent être vérifiés ;

9. l'emplacement des services de statut de validité des certificats qui peuvent être utilisés pour connaître le statut de validité du certificat qualifié.

Ces exigences peuvent être complétées par décret pris en Conseil des ministres, sur proposition du Ministère chargé de l'économie numérique.

Chapitre 10 : Restrictions extraordinaires

Article 476 Restrictions extraordinaires

Des mesures restreignant, au cas par cas, le libre exercice des activités encadrées par les dispositions du présent livre peuvent être prises par toute autorité gouvernementale, administrative ou judiciaire, lorsqu'il est porté atteinte ou qu'il existe un risque sérieux et grave d'atteinte au maintien de l'ordre ou de la sécurité publique, à la protection des personnes, à la protection des mineurs, à la santé publique ou à la préservation des intérêts de la défense nationale.

Livre Cinquième : Droit de la consommation

Titre 1 Droits des utilisateurs finals de réseaux et services de communications électroniques

Chapitre préliminaire : Application aux utilisateurs finals

Article 477 Application aux utilisateurs finals

Les dispositions du présent titre s'appliquent aux relations entre les opérateurs et tout consommateur ou tout organisme à but non lucratif, toute personne morale n'agissant pas à des fins professionnelles, ou toute petite entreprise, très petite entreprise ou microentreprise.

Chapitre 1 : Droit à la fourniture de services de communications électroniques et services connexes

Article 478 Droit à la fourniture de services de communications électroniques

Toute personne a droit aux services de communications électroniques.

Sauf décision prise en application d'une législation ou d'une réglementation nationale, toute personne physique ou morale qui remplit les conditions contractuelles et financières proposées par un opérateur pour la fourniture d'un service de communications électroniques ne peut se voir refuser la fourniture de ce service si elle en a formulé la demande.

Article 479 Droit à l'installation de lignes de communications électroniques dans un logement

Le propriétaire d'un immeuble ou son mandataire ne peut s'opposer à l'installation de la ligne raccordant son locataire ou occupant de bonne foi à un réseau de communications électroniques demandée par ce dernier dans le cadre de sa souscription à un service de communications électroniques.

Article 480 Dépôt de garantie

L'opérateur peut exiger de l'utilisateur final demandeur de services de communications électroniques un dépôt de garantie dont le montant est préalablement fixé et publié de manière transparente et non-discriminatoire.

La restitution des sommes versées au titre d'un dépôt de garantie est effectuée au plus tard dans un délai de ***trente (30) jours*** à compter de la restitution de l'objet garanti.

Article 481 Interdiction de déconnexion

Tout utilisateur final d'un service de communications électroniques qui respecte les conditions contractuelles et financières souscrites ne peut se voir déconnecter du réseau ou service de communications électroniques à moins qu'il en fasse la demande expresse, sauf en cas d'urgence ou pour des raisons de sécurité publique.

Article 482 Prohibition des limites aux droits des utilisateurs finals

Aucun opérateur ne peut limiter le droit d'un utilisateur final à :

1. choisir un fournisseur de biens ou de services ;

2. relier à son réseau de communications électroniques ouvert au public tout équipement radioélectrique ou équipement terminal bénéficiant d'un agrément à cet effet ;

3. relier à son réseau de communications électroniques ouvert au public tout réseau de communications électroniques interne qui répond aux normes et exigences en la matière.

Article 483 Egalité de traitement des utilisateurs finals, non-discrimination

Les opérateurs doivent respecter le principe d'égalité de traitement des utilisateurs finals. L'accès de ces derniers aux réseaux de communications électroniques ouverts au public doit être assuré dans des conditions objectives, transparentes et non discriminatoires.

Article 484 Fourniture obligatoire d'un service d'annuaire et de renseignements et d'un accès aux services d'urgence

Le service téléphonique offert par tout opérateur contient obligatoirement, sous une forme et selon des modalités fixées par l'Autorité de régulation, les services de renseignements et les services d'annuaire.

Les opérateurs qui fournissent un service téléphonique garantissent également un accès ininterrompu aux services d'urgence, conformément aux textes législatifs et réglementaires en vigueur et dans les conditions fixées par l'Autorité de régulation. Les opérateurs veillent notamment à ce qu'il soit possible de procéder gratuitement à des appels de secours et d'urgence à partir de tout poste fixe ou mobile connecté à leur réseau, y compris les cabines téléphoniques. Les moyens d'appel de secours mis à disposition dans les cabines téléphoniques doivent être faciles à manipuler.

Article 485 Protection des droits des personnes figurant dans les listes d'utilisateurs

L'établissement et la publication des listes d'utilisateurs de services téléphoniques s'effectue dans le respect de la protection des droits des personnes et en particulier des dispositions du Livre Premier.

Parmi les droits garantis, figurent ceux, pour toute personne :

1. d'être mentionnée ou de refuser d'être mentionnée sur les listes d'utilisateurs publiées dans les annuaires ou consultables par l'intermédiaire d'un service de renseignements ;

2. de s'opposer gratuitement à l'inscription de certaines données la concernant dans la mesure compatible avec les nécessités de la constitution des annuaires et des services de renseignements auxquels ces listes sont destinées ;

3. d'être informée préalablement des fins auxquelles sont établis, à partir de ces listes, des annuaires et services de renseignements et des possibilités d'utilisation reposant sur des fonctions de recherche intégrées à leur version électronique.

Le consentement préalable des utilisateurs de services téléphoniques mobiles est requis pour toute inscription de données à caractère personnel les concernant dans les listes d'utilisateurs destinées à être publiées dans les annuaires ou consultables par l'intermédiaire d'un service de renseignements.

Article 486 Portabilité des numéros

L'Autorité de régulation procède à des études de marché pour évaluer les besoins des utilisateurs finals en matière de portabilité des numéros afin d'identifier les catégories d'utilisateurs finals susceptibles de demander ce service. En cas de besoin clairement identifié, l'Autorité de régulation met en place un dispositif adapté pour permettre aux utilisateurs finals de conserver leur numéro et en définit les conditions de mise en œuvre.

L'Autorité de régulation peut imposer aux opérateurs la portabilité des numéros.

Article 487 Portabilité des courriers électroniques

Les opérateurs fournissant un service d'accès à Internet qui attribuent à leurs utilisateurs une adresse de courrier électronique dans le cadre de leur offre sont tenus de proposer à ces derniers, lorsqu'ils changent de fournisseur, une offre leur permettant de continuer, pour une durée de six (6) mois à compter de la résiliation, à avoir accès gratuitement aux courriers électroniques reçus sur l'adresse électronique attribuée sous son nom de domaine par ledit opérateur.

Article 488 Adaptation des obligations de fourniture d'information et de services aux personnes ayant des besoins spécifiques

Les dispositions du présent article s'appliquent vis-à-vis des personnes présentant un handicap entraînant des besoins spécifiques en matière de communications électroniques, en particulier les utilisateurs finals sourds, malentendants, aveugles ou aphasiques.

Les opérateurs prennent les mesures nécessaires pour fournir aux utilisateurs finals handicapés, à un tarif abordable, des produits et des services adaptés leur permettant de bénéficier d'un accès à tout ou partie des services de communications électroniques qu'ils fournissent équivalent à celui dont bénéficie la majorité des utilisateurs finals. Les opérateurs rendent accessibles leurs services dédiés à la clientèle aux utilisateurs finals handicapés par tout moyen adapté à leur handicap.

La mise en œuvre de cette obligation peut s'appuyer sur des applications de communications électroniques permettant la vocalisation du texte, la transcription de la voix en texte, la traduction en et depuis la langue des signes française ou la transcription en et depuis le langage parlé complété.

Les opérateurs assurent aux utilisateurs finals handicapés l'accès aux informations tarifaires, aux documents contractuels et de facturation par des moyens et sur des supports adaptés à leur handicap.

Les opérateurs mettent également en place une signalétique destinée à leurs clients indiquant les terminaux et services les mieux adaptés à chaque catégorie de handicap, évalués sur la base de critères objectifs et transparents.

Lorsque des offres des opérateurs prévoient la fourniture d'un équipement terminal, ceux-ci mettent à la disposition des utilisateurs finals handicapés des terminaux adaptés à leur handicap disponibles sur le marché. Les opérateurs tiennent également compte des besoins spécifiques des personnes handicapées dans la conception des équipements associés à leurs offres de services d'accès à Internet fixe.

Les opérateurs fournissant des services d'annuaire ou de renseignements fournissent un accès aux utilisateurs finals handicapés à ces services par un moyen adapté à leur handicap.

Les opérateurs prennent les mesures nécessaires pour fournir aux utilisateurs finals handicapés un accès aux services d'urgence équivalent à celui dont bénéficie la majorité des utilisateurs finals.

Article 489 Tarification des services de communications électroniques

Les tarifs sont fixés librement par les opérateurs sous réserve des dispositions du Titre 5 du Livre Deuxième et des mesures qui peuvent être imposées par l'Autorité de

régulation aux opérateurs ayant une puissance significative sur un marché du secteur des communications électroniques.

Les tarifs de raccordement, d'abonnement et des communications doivent respecter le principe d'égalité de traitement des utilisateurs final et être établis de manière à éviter une discrimination fondée sur la localisation géographique. Toutefois, en cas de difficultés exceptionnelles motivées par l'importance des surcoûts de mise en œuvre ou d'exploitation de certaines dessertes pour effectuer le raccordement de certains utilisateurs finals, les opérateurs peuvent pratiquer des conditions et tarifs de raccordement différenciés.

Chapitre 2 : Accès ouvert à Internet

Article 490 Accès ouvert à Internet

Les utilisateurs finals ont le droit d'accéder et de diffuser les informations et contenus légaux de leur choix, et d'utiliser et fournir des applications, services et équipements terminaux de leur choix sur les réseaux de communications électroniques, quel que soit le lieu où ils se trouvent et où se trouve le fournisseur, et quel que soit le lieu, l'origine ou la destination de l'information communiquée, du contenu diffusé, de l'application utilisée ou du service fourni ou utilisé.

Les opérateurs traitent tous trafics de façon égale et sans discrimination, restriction ou interférence, quels que soient l'expéditeur et/ou le destinataire, les contenus consultés et/ou diffusés, les applications et/ou les services utilisés ou fournis ou les équipements terminaux utilisés.

Les accords entre les opérateurs fournissant un service d'accès à Internet et les utilisateurs finals sur les conditions commerciales et techniques et les caractéristiques des services d'accès à Internet, telles que les prix, les volumes de données ou le débit, et toutes pratiques commerciales mises en œuvre par les opérateurs fournissant un accès à Internet, ne limitent pas l'exercice par les utilisateurs finals des droits énoncés au premier alinéa ni ne contreviennent aux principes énoncés par le deuxième alinéa.

Article 491 Mesures raisonnables de gestion du trafic

Les dispositions de l'Article 490 n'empêchent pas les opérateurs fournissant un service d'accès à Internet de mettre en œuvre des mesures raisonnables de gestion du trafic. Pour être réputées raisonnables, ces mesures doivent être transparentes, non-discriminatoires et proportionnées, et elles ne doivent pas être fondées sur des considérations commerciales, mais sur des différences objectives entre les exigences techniques en matière de qualité de service de certaines catégories spécifiques de trafic. Ces mesures ne peuvent concerner la surveillance de contenus particuliers et ne doivent pas être maintenues plus longtemps que nécessaire.

Les opérateurs fournissant un service d'accès à Internet n'appliquent pas de mesures de gestion du trafic qui vont au-delà de celles prévues au présent article et, en particulier, s'abstiennent de bloquer, de ralentir, de modifier, de restreindre, de perturber, de dégrader ou de traiter de manière discriminatoire des contenus, des applications ou des services spécifiques ou des catégories spécifiques de contenus, d'applications ou de services, sauf si nécessaire et seulement le temps nécessaire, pour :

1. se conformer aux textes législatifs et réglementaires en vigueur ou aux mesures donnant effet à ces textes, y compris les décisions des juridictions ou des autorités compétentes ;

2. préserver l'intégrité et la sûreté des réseaux, des services fournis par l'intermédiaire de ces réseaux et des équipements terminaux des utilisateurs finals ;

3. prévenir une congestion imminente du réseau et atténuer les effets d'une congestion exceptionnelle ou temporaire, pour autant que les catégories équivalentes de trafic fassent l'objet d'un traitement égal.

Article 492 Transparence des conditions d'accès à Internet

Les opérateurs fournissant un service d'accès à Internet veillent à ce que tout contrat incluant des services d'accès à Internet contienne au moins :

1. une explication claire et compréhensible, pour les réseaux fixes, sur le débit minimal normalement disponible ainsi que sur le débit maximal estimé et annoncé pour le téléchargement descendant et ascendant des services d'accès à Internet ou, pour les réseaux mobiles, sur le débit maximal estimé et annoncé pour le téléchargement descendant et ascendant des services d'accès à Internet ;
2. des informations sur la manière dont les mesures de gestion du trafic appliquées par l'opérateur concerné peuvent avoir une incidence sur la qualité des services d'accès à Internet, sur le respect de la vie privée des utilisateurs et sur la protection de leurs données à caractère personnel.

Article 493 Non-conformité des conditions d'accès à Internet

Tout écart significatif, permanent ou récurrent, entre les performances réelles des services d'accès à Internet en matière de débit ou d'autres paramètres de qualité de service et les performances indiquées par l'opérateur dans le contrat avec l'utilisateur final, est réputé constituer une performance non-conforme pouvant donner lieu à réclamation par l'utilisateur final lorsque cet écart est constaté par un mécanisme de surveillance mis en œuvre ou agréé par l'Autorité de régulation.

Chapitre 3 : Information des utilisateurs finals et contrats

Article 494 Transparence et publicité des offres et tarifs

Les opérateurs publient régulièrement et mettent à disposition des utilisateurs finals dans leurs points de vente et sur leur site Internet des informations claires, transparentes, facilement accessibles et actualisées relatives à l'ensemble des services proposés, aux tarifs pratiqués ainsi qu'aux conditions générales de vente et/ou de services, ainsi que les contrats types prévus par l'Article 496.

Article 495 Informations fournies aux utilisateurs finals

Les informations visées à l'Article 494 incluent :

1. les informations visées aux Article 362, Article 366, Article 367 et Article 370;
2. les informations visées à l'Article 496 ;
3. les produits et services destinés aux utilisateurs finals handicapés ;
4. les conséquences juridiques de l'utilisation des services de communications électroniques pour se livrer à des activités illicites ou diffuser des contenus préjudiciables, en particulier lorsqu'ils peuvent porter atteinte au respect des droits et des libertés d'autrui ;
5. les moyens de protection contre les risques d'atteinte à la sécurité individuelle, à la vie privée et aux données à caractère personnel lors de l'utilisation des services de communications électroniques.

Article 496 Contrats-types conclus avec les utilisateurs finals

Tout opérateur élabore des contrats types et leurs avenants pour la fourniture de ses services aux utilisateurs finals. Ces contrats types contiennent les informations suivantes sous une forme claire, détaillée et aisément accessible :

1. l'identité et l'adresse de l'opérateur ;
2. les services offerts, leur niveau de qualité et le délai nécessaire pour en assurer la fourniture ;
3. le détail des tarifs pratiqués, notamment les frais de résiliation, les modes de paiement proposés et leurs conditions ;
4. la durée du contrat, les conditions de renouvellement et d'interruption des services et du contrat ;

5. les services après-vente fournis, ainsi que les modalités permettant de solliciter la fourniture de ces services ;

6. les restrictions apportées à l'accès à des services et à leur utilisation, ainsi qu'à celle des équipements terminaux fournis, dans le respect des dispositions du présent titre ;

7. les possibilités qui s'offrent à l'utilisateur final de faire figurer ou non ses données à caractère personnel dans un annuaire et les données concernées ;

8. le type de mesure qu'est susceptible de prendre l'opérateur afin de réagir à une atteinte ou un risque d'atteinte à la sécurité ou à l'intégrité de son réseau.

Article 497 Modification des conditions contractuelles

Les opérateurs ne peuvent unilatéralement modifier les termes d'un contrat qui les lient aux utilisateurs finals que :

1. pour les raisons indiquées dans les termes du contrat et conformément à ce dernier ; ou

2. sur la base d'une modification des textes législatifs et réglementaires en vigueur ou d'une décision des juridictions ou autorités compétentes.

Tout projet de modification des conditions contractuelles de fourniture d'un service de communications électroniques est communiqué par l'opérateur à l'utilisateur final par écrit ou sur un autre support durable à la disposition de ce dernier au moins ***un (1) mois*** avant son entrée en vigueur, assorti de l'information selon laquelle l'utilisateur final peut, tant qu'il n'a pas expressément accepté les nouvelles conditions, résilier le contrat sans pénalité de résiliation et sans droit à dédommagement, jusqu'au terme d'un délai de ***quatre (4) mois*** après la communication des nouvelles dispositions contractuelles.

La modification ne prend effet qu'à l'issue de ce délai de ***quatre (4) mois***, à moins que l'utilisateur final n'ait expressément accepté les modifications communiquées, auquel cas les nouvelles dispositions contractuelles prennent effet à la date de l'acceptation formulée par l'utilisateur final.

Les dispositions du présent article ne s'appliquent pas dans les cas suivants :

1. les modifications contractuelles envisagées sont toutes exclusivement au bénéfice de l'utilisateur final sans aucune incidence négative pour lui ;

2. les modifications contractuelles envisagées ont un caractère purement administratif et n'ont pas d'incidence négative pour l'utilisateur final ;

3. les modifications contractuelles envisagées sont directement imposées par la loi.

Article 498 Poursuite à titre onéreux de services accessoires initialement fournis gratuitement

La poursuite à titre onéreux de la fourniture de services accessoires à un contrat principal de communications électroniques comprenant une période initiale de gratuité est soumise à l'accord exprès de l'utilisateur final à qui ces services sont proposés.

Article 499 Résiliation

La durée du préavis de résiliation par un utilisateur final d'un contrat de services de communications électroniques ne peut excéder dix (10) jours à compter de la réception par l'opérateur de la demande de résiliation.

L'utilisateur final peut toutefois demander que cette résiliation prenne effet plus de dix (10) jours après la réception de sa demande de résiliation par l'opérateur.

Article 500 Prescription

La prescription est acquise au profit des opérateurs dans leurs relations contractuelles avec les utilisateurs finals en matière de demandes en restitution du prix des prestations de communications électroniques fournies après un délai ***d'un (1) an*** à compter du jour du paiement desdites prestations.

La prescription est acquise au profit des utilisateurs finals dans leurs relations contractuelles avec les opérateurs pour les sommes dues en paiement des prestations de communications électroniques reçues lorsque les opérateurs ne les ont pas réclamées dans un délai ***d'un (1) an*** à compter de la date de leur exigibilité.

Chapitre 4 : Gestion des données à caractère personnel des utilisateurs finals

Article 501 Effacement ou anonymisation des données relatives au trafic

Sans préjudice des dispositions du Livre Premier, les dispositions du présent chapitre s'appliquent au traitement des données à caractère personnel dans le cadre de l'exploitation de réseaux de communications électroniques ouverts au public et de la fourniture au public de services de communications électroniques. Elles s'appliquent notamment aux réseaux et services qui comportent un dispositif de collecte de données et d'identification.

Les opérateurs effacent ou rendent anonyme toute donnée relative au trafic, sous réserve des dispositions du présent chapitre.

Les opérateurs établissent, dans le respect des dispositions du présent chapitre, des procédures internes permettant de répondre aux demandes des autorités compétentes, notamment celles présentées dans le cadre de l'Article 174 .

Les personnes qui, au titre d'une activité professionnelle principale ou accessoire, offrent au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès à un réseau, y compris à titre gratuit, sont soumises au respect des dispositions applicables en vertu du présent article.

Article 502 Nature des données techniques concernées

Les données conservées et traitées dans les conditions définies au présent chapitre portent exclusivement sur l'identification des utilisateurs finals, sur les caractéristiques techniques des communications assurées par les opérateurs et sur la localisation des équipements terminaux.

Elles ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications.

La conservation et le traitement de ces données s'effectuent dans le respect des dispositions du Livre Premier.

Les opérateurs prennent toutes les mesures nécessaires pour empêcher une utilisation de ces données à des fins autres que celles prévues au présent chapitre.

Article 503 Traitement particulier des données de localisation

Sans préjudice des dispositions du présent chapitre et sous réserve des nécessités d'enquêtes judiciaires et de police, ou pour les besoins de la sécurité publique ou de la défense nationale, les données permettant de localiser l'équipement terminal d'un utilisateur final ne peuvent ni être utilisées pendant la communication à des fins autres que son acheminement, ni être conservées ou traitées après l'achèvement de la communication à moins d'avoir préalablement recueilli le consentement de l'utilisateur final dûment informé des catégories de données en cause, de la durée du traitement, de ses fins et du fait que ces données seront ou non transmises à des tiers.

L'utilisateur final peut suspendre ou retirer son consentement à tout moment par un moyen simple et gratuit, hormis les coûts liés à la communication du retrait ou de la suspension dudit consentement.

Tout appel destiné à un service d'urgence vaut consentement de l'utilisateur final au sens de l'alinéa précédent jusqu'à l'aboutissement de l'opération de secours qu'il déclenche et seulement pour en permettre la réalisation.

Article 504 Exceptions aux fins de communication aux autorités judiciaires

Les opérations tendant à effacer ou à rendre anonymes certaines catégories de données relatives au trafic peuvent être différées pour une durée maximale de deux (2) ans en vue

de leur communication aux autorités judiciaires conformément à l'Article 174 et dans les conditions prévues par les textes législatifs et réglementaires en vigueur.

Un décret pris en Conseil des ministres après avis de l'Autorité de régulation multisectorielle de Djibouti et de la Commission Nationale de Protection des Données à Caractère Personnel, détermine dans les limites fixées par l'Article 502, ces catégories de données et la durée de leur conservation, selon l'activité des opérateurs et la nature des communications.

Article 505 Exceptions aux fins de facturation des services de communications électroniques

Pour les besoins de la facturation et du paiement des prestations de communications électroniques, les opérateurs peuvent, jusqu'à la fin de la période au cours de laquelle la facture peut être légalement contestée ou des poursuites engagées pour en obtenir le paiement, utiliser, conserver et, le cas échéant, transmettre à des tiers directement concernés par la facturation ou le recouvrement de ces sommes, les catégories de données techniques déterminées par un décret pris en Conseil des ministres après avis de l'Autorité de régulation multisectorielle de Djibouti et de la Commission Nationale de Protection des Données à Caractère Personnel, dans les limites fixées par l'Article 502 et selon l'activité des opérateurs et la nature de la communication.

Article 506 Exceptions aux fins de commercialisation de services de communications électroniques ou de fourniture de services à valeur ajoutée

Les opérateurs peuvent réaliser un traitement des données relatives au trafic, déterminées par un décret pris en Conseil des ministres après avis de l'Autorité de régulation multisectorielle de Djibouti et de la Commission Nationale de Protection des Données à Caractère Personnel et dans les limites fixées par l'Article 502, en vue de commercialiser leurs propres services de communications électroniques ou de fournir des services à valeur ajoutée, si les utilisateurs y ont préalablement et expressément consenti, et pour une durée déterminée. Cette durée ne peut, en aucun cas, être supérieure à la période nécessaire pour la fourniture ou la commercialisation de ces services.

Article 507 Exceptions aux fins de sécurité des réseaux

Les opérateurs peuvent conserver certaines données déterminées par un décret pris en Conseil des ministres après avis de l'Autorité de régulation multisectorielle de Djibouti et de la Commission Nationale de Protection des Données à Caractère Personnel, et dans les limites fixées par l'Article 502 , en vue d'assurer la sécurité de leurs réseaux.

Article 508 Sanctions

Est puni de 10 ans d'emprisonnement et de 8.500.000 DJF d'amende le fait pour un opérateur ou ses agents :

1. de ne pas procéder aux opérations tendant à effacer ou à rendre anonymes les données relatives aux communications dans les cas où ces opérations sont prescrites par la loi ;

2. de ne pas procéder à la conservation des données relatives au trafic dans les conditions où cette conservation est exigée par la loi.

Les personnes physiques coupables de ces infractions encourent également l'interdiction, pour une durée de cinq (5) ans au plus, d'exercer l'activité professionnelle à l'occasion de laquelle l'infraction a été commise.

Chapitre 5: Surveillance, réclamations, sanctions

Article 509 Surveillance par l'Autorité de régulation

L'Autorité de régulation surveille étroitement l'application des dispositions du présent titre, veille au respect de ces dispositions et encourage la disponibilité permanente de services d'accès à Internet non-discriminatoires à des niveaux de qualité qui correspondent à l'état d'avancement des technologies.

À cette fin, l'Autorité de régulation peut imposer des exigences concernant des caractéristiques techniques, des exigences minimales de qualité du service et d'autres mesures adaptées et nécessaires aux opérateurs.

Les opérateurs communiquent les informations demandées dans les délais et selon le degré de précision exigés par l'Autorité de régulation.

À la demande de l'Autorité de régulation, les opérateurs fournissant un service d'accès à Internet mettent à sa disposition les informations relatives aux obligations énoncées au Chapitre 2 du présent titre, notamment les informations concernant la gestion de la capacité de leur réseau et du trafic, ainsi que les justifications de toute mesure de gestion du trafic appliquée.

Article 510 Mise en place d'un système transparent de traitement des réclamations

Les opérateurs établissent et gèrent un système transparent de traitement des réclamations des utilisateurs finals.

Les opérateurs fournissant un service d'accès à Internet établissent des procédures spécifiques transparentes, simples et efficaces pour traiter les réclamations des

utilisateurs finals concernant les droits et les obligations spécifiquement énoncés à l'Article 490.

Les réclamations sont traitées par les opérateurs dans un délai n'excédant pas ***un (1) mois***.

Les opérateurs conservent une copie ou une retranscription des échanges relatifs aux réclamations et à leur traitement permettant leur réutilisation en conformité avec les dispositions du Livre Premier et du Titre 1 du Chapitre 4 du présent livre.

Titre 2 Publicité par voie électronique et prospection directe

Chapitre 1 : Publicité par voie électronique

Article 511 Identification et transparence de la publicité par voie électronique

Toute publicité, sous quelque forme que ce soit, accessible par un service de communications électroniques ou un service de communication au public en ligne, doit pouvoir être clairement identifiée comme telle. Elle doit rendre clairement identifiable son expéditeur ainsi que la personne physique ou morale pour le compte de laquelle elle est réalisée.

La publicité peut notamment être identifiée comme telle en raison de son titre, de sa présentation ou de son objet. À défaut, elle comporte la mention « publicité » de manière claire, lisible, apparente et non-équivoque.

Les conditions pour bénéficier d'offres et d'opérations promotionnelles ou pour participer à des concours ou des jeux promotionnels, lorsque ces offres, concours ou jeux sont proposés par voie électronique, doivent être aisément accessibles et présentées de manière claire, précise et non-équivoque.

Article 512 Identification et transparence de la publicité adressée par courrier électronique

Les publicités adressées par courrier électronique, notamment les offres et opérations promotionnelles telles que les rabais, primes ou cadeaux de quelque nature qu'ils soient, ainsi que les concours ou les jeux promotionnels, doivent pouvoir être identifiées comme telles de manière claire et non équivoque dès leur réception par leur destinataire, ou en cas d'impossibilité technique, dans le corps du message.

Ces messages indiquent une adresse ou un moyen électronique permettant effectivement au destinataire de transmettre une demande visant à obtenir que ces publicités ne lui soient plus adressées.

Article 513 Sanctions

Tout manquement aux obligations prévues par le présent chapitre est puni de 30 jours à 6 mois] d'emprisonnement et de 35.000 DJF à 350.000 DJF d'amende dans les conditions prévues par le Code de commerce.

Chapitre 2 : Prospection directe

Article 514 Consentement à la prospection directe

La prospection directe au moyen de systèmes automatisés de communications électroniques, de réseaux, services et/ou terminaux de communications électroniques, télécopieurs, courriers électroniques ou SMS utilisant les données à caractère personnel d'un utilisateur qui n'a pas préalablement exprimé son consentement à recevoir des prospections directes par ces moyens, est interdite.

La charge de la preuve du consentement du destinataire de la prospection directe incombe à la personne physique ou morale à l'origine de la prospection.

Pour l'application du présent chapitre, les appels et messages ayant pour objet d'inciter l'utilisateur à appeler un numéro surtaxé ou à envoyer un message textuel surtaxé relèvent de la prospection directe.

Pour les besoins du présent chapitre, le consentement à la prospection directe doit être conforme aux caractéristiques définies par l'Article 57 et être recueilli dans des conditions conformes à l'Article 58.

Article 515 Exceptions au consentement à la prospection directe

La prospection directe est autorisée sans le consentement préalable du destinataire personne physique, si l'ensemble des conditions suivantes sont remplies :

1. les coordonnées du destinataire ont été recueillies auprès de lui en toute connaissance de cause, et dans le respect des dispositions du Livre Premier, à l'occasion d'une vente ou d'une prestation de services ;

2. la prospection directe concerne exclusivement des produits ou services analogues proposés par le même fournisseur ;

3. le destinataire se voit offrir, de manière simple, expresse et dénuée d'ambiguïté, la possibilité de s'opposer sans frais à l'utilisation de ses coordonnées, au moment où elles sont recueillies et chaque fois qu'un message de prospection lui est adressé, au cas où il n'aurait pas préalablement refusé une telle exploitation.

La prospection directe est autorisée sans le consentement préalable du destinataire personne morale.

Par exception, la prospection directe est également autorisée sans le consentement préalable du destinataire personne physique uniquement si le message est adressé à son adresse électronique professionnelle, et si cette personne est prospectée au titre de la fonction qu'elle occupe.

Article 516 Obligation d'information

Il est interdit d'émettre à des fins de prospection directe des messages au moyen de systèmes automatisés de communications électroniques, de réseaux, services et/ou terminaux de communications électroniques, télécopieurs, courriers électroniques ou SMS, sans indiquer les moyens et les coordonnées valables auxquelles le destinataire peut utilement transmettre une demande tendant à obtenir sans frais, que ces communications cessent.

Il est également interdit de dissimuler l'identité de la personne pour le compte de laquelle la communication est émise, notamment en :

1. utilisant l'adresse électronique ou l'identité d'un tiers ;

2. falsifiant ou masquant toute information permettant d'identifier l'origine du message ou son chemin de transmission ;

3. mentionnant un objet sans rapport avec les biens ou services proposés ;

4. encourageant le destinataire des messages à visiter des sites internet de tiers.

La Commission nationale de protection des données à caractère personnel veille, pour ce qui concerne la prospection directe utilisant les coordonnées d'un utilisateur personne physique, au respect des dispositions du présent chapitre dans les conditions prévues au Livre Premier . A cette fin, elle peut notamment recevoir, par tous moyens, les plaintes relatives aux manquements aux dispositions du présent chapitre.

Article 517 Droit d'opposition

Tout destinataire d'une prospection directe peut notifier directement à toute personne qui propose la fourniture de biens ou de services en ligne, sans justification et sans frais, sa volonté de ne plus recevoir de prospection directe.

Dans ce cas la personne proposant la fourniture de biens ou de services en ligne est tenue de :

1. délivrer sans délai un accusé de réception par tout moyen, y compris par voie électronique, confirmant au destinataire de la prospection directe l'enregistrement de sa demande ;

2. prendre, dans un délai raisonnable, les mesures nécessaires pour respecter la volonté du destinataire de la prospection directe ;

3. tenir à jour la liste des destinataires qui ont exprimé leur volonté de ne plus recevoir de prospections directes de sa part.

Article 518 Renforcement de la protection des personnes vulnérables

Lorsque la prospection directe est destinée aux enfants, aux personnes âgées, aux personnes malades ou vulnérables, ou à toute personne qui ne serait pas en mesure de comprendre pleinement les informations qui lui sont présentées, les exceptions prévues au présent livre doivent être interprétées plus strictement.

Article 519 Sanctions

Quiconque fait de la prospection directe au moyen d'un automate d'appel, d'un télécopieur ou d'un courrier électronique utilisant, sous quelque forme que ce soit, les coordonnées d'une personne physique qui n'a pas exprimé son consentement préalable à recevoir ladite prospection est punie de 6 à 12 mois d'emprisonnement et de 350.000 DJF à 1.400.000 DJF d'amende.

Toute personne effectuant de la prospection directe en violation des autres dispositions du présent chapitre est punie de 30 jours à 6 mois d'emprisonnement et de 35.000 DJF à 350.000 DJF d'amende.

Lorsque ces manquements concernent la prospection directe destinée à des enfants, des personnes âgées, des personnes malades ou vulnérables, ou à toute personne qui ne serait pas en mesure de comprendre pleinement les informations qui lui sont présentées, les peines prévues sont doublées.

Titre 3 Protection en matière de contrats conclus par voie électronique

Chapitre préliminaire : Responsabilité du professionnel à l'égard du consommateur, livraison et transfert des risques

Article 520 Responsabilité de plein droit du professionnel

Le professionnel est responsable de plein droit à l'égard du consommateur de la bonne exécution des obligations résultant du contrat conclu par voie électronique en vertu des dispositions énoncées à l'Article 371.

Article 521 Délai d'exécution des services et de livraison des biens

Sous réserve d'un autre délai convenu de manière expresse entre les parties, le professionnel exécute la commande et le cas échéant livre les biens ou exécute les

services sans retard injustifié, et au plus tard dans un délai de trente (30) jours à compter de la conclusion du contrat.

La livraison s'entend de la réalisation effective du service, ou du transfert au consommateur de la possession physique ou du contrôle des biens.

Article 522 Transfert des risques

Tout risque de perte ou d'endommagement des biens objet de la commande est transféré au consommateur au moment où ce dernier, ou un tiers désigné par lui et autre que le transporteur proposé par le professionnel, prend physiquement possession de ces biens.

Chapitre 1 : Droit de rétractation du consommateur et résolution du contrat

Article 523 Délai de rétractation

Le consommateur dispose d'un délai de quatorze (14) jours pour se rétracter d'un contrat conclu par voie électronique. Ce droit de rétractation s'exerce sans justification et sans frais autres que les éventuels coûts directs de renvoi du bien au professionnel, le cas échéant.

Si les informations prévues aux Article 362, Article 366, Article 367 et Article 370 sont communiquées au consommateur avant la conclusion du contrat, le délai d'exercice du droit de rétractation commence à courir :

1. s'agissant des contrats portant sur la fourniture de biens, à compter du lendemain de la date à laquelle le consommateur, ou un tiers désigné par lui autre que le transporteur désigné ou non par le professionnel, réceptionne le bien;

2. s'agissant des contrats portant sur la fourniture de services, à compter du lendemain du jour de la conclusion du contrat.

Si le professionnel manque à son obligation d'information préalable prévue aux Article 362,Article 366, Article 367 et Article 370, le délai d'exercice du droit de rétractation est porté à trois (3) mois. Si la fourniture de ces informations intervient pendant cette prolongation, le délai de rétractation expire au terme d'une période de quatorze (14) jours à compter du jour où le consommateur a reçu ces informations.

Dans le cas d'une commande portant sur plusieurs biens livrés séparément ou dans le cas d'une commande d'un bien composé de lots ou de pièces multiples dont la livraison est échelonnée sur une période définie, le délai court à compter de la réception du dernier bien ou lot ou de la dernière pièce.

Pour les contrats prévoyant la livraison régulière de biens pendant une période définie, le délai court à compter de la réception du premier bien.

Article 524 Effets de la rétractation

L'exercice du droit de rétractation met fin à l'obligation des parties soit d'exécuter le contrat, soit de le conclure lorsque le consommateur a fait une offre.

L'exercice du droit de rétractation d'un contrat principal conclu à distance ou hors établissement met automatiquement fin à tout contrat accessoire.

Article 525 Modalités d'exercice du droit de rétractation

L'exercice du droit de rétractation par le consommateur suppose qu'il ait eu la possibilité de raisonnablement essayer le bien commandé, en vue de s'assurer de sa conformité. Cette disposition ne s'applique pas aux services dont l'exécution est effectuée en une fois.

Le consommateur notifie au professionnel sa décision de se rétracter par la transmission d'un formulaire de rétractation proposé par le professionnel ou par courrier postal ou électronique avec accusé de réception dans le délai prévu par l'Article 523. Le professionnel peut également permettre au consommateur de remplir et de transmettre en ligne, sur son site internet, le formulaire ou la notification de rétractation, auquel cas, le professionnel communique sans délai au consommateur un accusé de réception de la rétractation sur un support durable.

En cas d'exercice du droit de rétractation, le consommateur doit cesser sans délai l'utilisation du bien ou du service fourni.

En cas d'exercice du droit de rétractation pour les contrats portant sur la fourniture de biens, le consommateur est tenu de renvoyer le bien au professionnel sans retard excessif et au plus tard dans un délai de quatorze (14) jours suivant la notification de sa décision de rétractation au professionnel, sauf à ce que le professionnel propose de reprendre lui-même le bien ou offre de prendre les frais de retour du bien à sa charge. Le consommateur ne supporte que les coûts directs de renvoi des biens, sauf si le professionnel accepte de les prendre à sa charge ou s'il a omis d'informer le consommateur que ces coûts sont à sa charge.

La charge de la preuve de l'exercice du droit de rétractation pèse sur le consommateur.

Article 526 Principe de remboursement par le professionnel

En cas d'exercice du droit de rétractation, le professionnel est tenu de rembourser toutes les sommes déjà versées par le consommateur, y compris les frais de livraison, sous réserve des dispositions énoncées à l'Article 527 et à l'Article 528.

Ce remboursement intervient sans retard injustifié et au plus tard dans un délai de trente (30) jours, à compter de la date de réception par le professionnel du bien retourné pour les contrats portant sur la fourniture de biens, et à compter de la date de notification de la rétractation pour les contrats portant sur la fourniture de services.

Si le remboursement n'est pas effectué dans ce délai, les sommes dues au consommateur sont de plein droit majorées au taux d'intérêt légal, à compter du lendemain de l'expiration du délai.

Le professionnel peut s'opposer à la réception du bien retourné et au remboursement du consommateur en raison de la dépréciation du bien, si cette dépréciation résulte de manipulations effectuées par le consommateur autres que celles strictement nécessaires pour vérifier sa conformité ou dépassant manifestement l'usage fait à titre de test ou d'essai.

Article 527 Remboursement de la commande

Le remboursement de la commande s'effectue sans frais pour le consommateur, dans les mêmes conditions et par les mêmes moyens de paiement que ceux utilisés pour le paiement de sa commande, sauf accord exprès du consommateur et pour autant que l'utilisation d'un autre mode de remboursement n'occasionne pas de frais supplémentaires au consommateur.

Article 528 Remboursement des frais de livraison

Les frais de livraisons sont remboursés au consommateur si le droit de rétractation est exercé en raison :

1. d'un dépassement du délai de livraison par le professionnel ;

2. d'un manquement du professionnel à l'une quelconque de ses obligations contractuelles ou de celles prévues par les dispositions du présent titre et des dispositions du Livre Quatrième Titre 1 et Titre 2.

Si le droit de rétractation est exercé pour d'autres raisons, le professionnel n'est pas tenu de rembourser les frais de livraison au consommateur.

Article 529 Aménagements du droit de rétractation pour les services

Si le consommateur souhaite que la fourniture du service commence avant la fin du délai de rétractation, le professionnel recueille son accord préalable exprès sur support durable.

En cas d'exercice du droit de rétractation d'un contrat de prestation de service dont l'exécution a commencé avant l'expiration du délai de rétractation à la demande du consommateur, le consommateur est tenu au paiement de la partie du prix déterminée

proportionnellement au service effectivement fourni entre le jour du début de la fourniture du service et le jour de sa notification d'exercice du droit de rétractation.

Le consommateur perd son droit de rétractation dans le cadre de contrats portant sur la fourniture de services si le service a été fourni dans sa totalité et lorsque l'exécution du contrat a commencé avec l'accord préalable du consommateur ayant pris acte qu'il perdrait son droit de rétractation.

Le consommateur qui a exercé son droit de rétractation d'un contrat de fourniture de contenu numérique non fourni sur un support matériel n'est redevable d'aucune somme si le professionnel n'a pas recueilli son accord préalable exprès pour l'exécution du contrat avant la fin du délai de rétractation ainsi que la preuve de son renoncement à son droit de rétractation, ou si le contrat ne reprend pas les mentions prévues aux Article 362,Article 366, Article 367 et Article 370.

Article 530 Exceptions au droit de rétractation pour certains biens

Le consommateur ne peut exercer de droit de rétractation pour les contrats conclus par voie électronique portant sur :

1. des services pleinement exécutés avant la fin du délai de rétractation et dont l'exécution a commencé après accord préalable exprès du consommateur et renoncement exprès à son droit de rétractation ;

2. des biens ou des services dont le prix dépend de fluctuations sur le marché financier échappant au contrôle du professionnel et susceptibles de se produire pendant le délai de rétractation ;

3. des biens confectionnés sur-mesure ou suivant les spécifications du consommateur ou nettement personnalisés par ce dernier ;

4. des biens qui, par leur nature, sont susceptibles de se détériorer ou de se périmer rapidement, tels que les denrées alimentaires et boissons ;

5. des biens qui ont été descellés par le consommateur après la livraison et qui ne peuvent être renvoyés pour des raisons d'hygiène ou de protection de la santé ;

6. des biens qui, après avoir été livrés, et de par leur nature, sont mélangés de manière indissociable avec d'autres articles ;

7. des travaux d'entretien ou de réparation à réaliser en urgence au domicile du consommateur et expressément sollicités par lui, dans la limite des pièces de rechange et travaux strictement nécessaires pour répondre à l'urgence ;

8. des prestations de services d'hébergement autres que d'hébergement résidentiel, de services de transport de biens, de locations de voitures, de restauration ou

d'activités de loisirs qui doivent être fournis à une date ou à une période déterminée ;

9. des contenus numériques, enregistrements audio ou vidéo ou logiciels informatiques descellés par le consommateur après la livraison ;

10. un contenu numérique non fourni sur un support matériel dont l'exécution a commencé après accord préalable exprès du consommateur et renoncement exprès à son droit de rétractation ;

11. des journaux, périodiques ou magazines, sans préjudice du droit du consommateur de résilier les contrats d'abonnement à ces publications ;

12. des biens acquis dans le cadre d'enchères publiques.

Article 531 Résolution du contrat de crédit interdépendant

Lorsque l'opération d'achat est entièrement ou partiellement couverte par un crédit accordé au consommateur par le vendeur ou par un tiers sur la base d'un contrat conclu entre le vendeur et le tiers, la rétractation du consommateur entraîne la résolution, sans pénalité, du contrat de crédit.

Article 532 Droit de résolution

En cas de dépassement du délai d'exécution de la commande ou de livraison des biens selon les dispositions énoncées à l'Article 521, le consommateur peut obtenir la résolution de plein droit du contrat par notification adressée au professionnel par courrier postal avec accusé de réception ou par courrier électronique. Le contrat est considéré comme résolu à la réception par le professionnel de la notification de résolution, à moins que le professionnel ne se soit exécuté entre-temps.

En cas de résolution du contrat par le consommateur conformément aux dispositions du présent article, le professionnel est tenu de lui rembourser les sommes versées au titre du contrat dans un délai de trente (30) jours à compter de la réception de la notification de résolution, et sous réserve des dispositions énoncées à l'Article 526.

Chapitre 2 : Garantie légale de conformité

Article 533 Application de la garantie légale de conformité au commerce électronique

Toute personne exerçant une activité de commerce électronique en République de Djibouti ou à destination de consommateurs situés sur le territoire de la République de Djibouti répond des défauts de conformité existant à la livraison des biens.

Elle répond également des défauts de conformité résultant de l'emballage, des instructions de montage ou de l'installation lorsque ceux-ci ont été mis à sa charge par le contrat ou ont été réalisés sous sa responsabilité.

La garantie légale de conformité s'applique aux contrats portant sur la vente de biens ou sur la fourniture de biens à fabriquer ou à produire.

Article 534 Contrats et biens exclus de la garantie légale de conformité

La garantie légale de conformité ne s'applique pas aux biens vendus aux enchères publiques ou par un huissier.

Elle ne s'applique pas non plus aux biens fournis dans le cadre d'un contrat entre professionnels ou entre particuliers.

Article 535 Conditions de conformité des biens

Un bien est conforme à la commande :

1. s'ilest propre à l'usage habituellement attendu d'un bien semblable et, le cas échéant :

   a) s'il correspond à la description donnée par le vendeur dans son offre et possède les qualités que celui-ci a présentées au consommateur ;

   b) s'il présente les qualités qu'un consommateur peut légitimement attendre eu égard aux déclarations publiques faites par le vendeur, par le producteur ou par son représentant, notamment dans la publicité ;

2. ou s'il présente les caractéristiques définies d'un commun accord par les parties ou est propre à tout usage spécial recherché par le consommateur, porté à la connaissance du vendeur et que ce dernier a accepté.

Article 536 Délais et modalités d'exercice de la garantie

Le consommateur dispose d'un délai de quatorze (14) jours à partir de la livraison du bien pour dénoncer sa non-conformité au vendeur. Cette dénonciation est faite par courrier postal avec accusé de réception ou par courrier électronique.

Les défauts de conformité qui apparaissent dans un délai de vingt-quatre (24) mois à partir de la livraison du bien sont présumés exister au moment de la livraison, sauf preuve contraire. Pour les biens vendus d'occasion, ce délai est fixé à six (6) mois.

Le vendeur peut combattre cette présomption si celle-ci n'est pas compatible avec la nature du bien ou le défaut de conformité invoqué.

Article 537 Exception en cas de connaissance du défaut

Le consommateur ne peut contester la conformité du bien en invoquant un défaut qu'il connaissait ou ne pouvait ignorer à la passation de la commande. Il en va de même lorsque le défaut tire son origine dans les matériaux que le consommateur a lui-même fournis pour fabriquer ou produire le bien commandé.

Article 538 Modes de remédiation au défaut

En cas de défaut de conformité, le consommateur a le choix, sans frais, entre la réparation et le remplacement du bien.

Toutefois, le vendeur peut ne pas procéder selon le choix de l'acquéreur si ce choix lui fait supporter un coût manifestement disproportionné au regard de l'autre modalité et compte tenu de la valeur du bien ou de l'importance du défaut. Le vendeur est alors tenu de procéder, sauf impossibilité, selon la modalité de son choix et ce en dépit du choix initial du consommateur.

Si la réparation ou le remplacement du bien sont impossibles, le consommateur peut, sans frais, retourner le bien au vendeur et se faire rembourser la totalité du prix, ou conserver le bien et se faire rembourser une partie du prix. La même faculté lui est ouverte si la réparation ou le remplacement du bien, qu'elle soit demandée par le consommateur, proposée par le vendeur ou convenue entre les parties, ne peut être mise en œuvre dans un délai d'un (1) mois suivant la réclamation du consommateur ou si la réparation ou le remplacement du bien ne peut être mise en œuvre sans inconvénient majeur pour le consommateur compte tenu de la nature du bien et de l'usage qu'il recherche.

Les dispositions du présent article ne font pas obstacle à l'allocation de dommages et intérêts.

Article 539 Prescription

L'action résultant du défaut de conformité est prescrite après un délai de deux (2) ans à compter de la livraison du bien.

Chapitre 3 : Garantie des vices cachés

Article 540 Application de la garantie des vices cachés au commerce électronique

Toute personne exerçant une activité de commerce électronique en République de Djibouti ou à destination de personnes situées sur le territoire de la République de Djibouti garantit les biens vendus contre les vices cachés qui les rendent impropre à

l'usage auquel on les destine, ou qui diminuent tellement cet usage que l'acquéreur ne les aurait pas acquis ou n'en aurait donné qu'un moindre prix, s'il les avait connus.

La garantie des vices cachés s'applique aux contrats portant sur la vente ou la fourniture de biens mobiliers ou immobiliers, et conclus entre professionnels, entre particuliers, ou entre un professionnel et un particulier.

Article 541 Exception en cas de vices apparents

Le vendeur n'est pas tenu des vices apparents et que l'acquéreur a pu lui-même constater.

Article 542 Vices cachés inconnus du vendeur

Le vendeur est tenu de garantir les vices cachés du bien même s'il n'en avait pas connaissance au moment de la commande, à moins qu'il n'ait stipulé que dans ce cas il ne sera obligé à aucune garantie.

Article 543 Modes de remédiation aux vices cachés découverts

En cas de découverte de vices cachés après la livraison du bien, l'acquéreur a le choix, sans frais, entre :

1. conserver le bien et se faire rembourser une partie du prix par le vendeur ;

2. retourner le bien au vendeur et se faire rembourser la totalité du prix ;

3. retourner le bien au vendeur et se faire livrer un nouveau bien, exempt de vices.

Il n'y a pas lieu à résolution du contrat ou à diminution du prix si le vendeur s'oblige à réparer les vices cachés.

Article 544 Remboursement de l'acquéreur par le vendeur

Selon le choix opéré par l'acquéreur en vertu de l'Article 543, le vendeur est tenu de restituer tout ou partie du prix versé par l'acquéreur.

Si le vendeur ignorait les vices du bien et n'a stipulé aucune exclusion au titre de la garantie des vices cachés, il n'est tenu qu'à la restitution du prix et au remboursement à l'acquéreur des frais occasionnés par la vente.

Si le vendeur avait connaissance des vices du bien, il est tenu, outre la restitution du prix qu'il en a reçu et des frais occasionnés par la vente, de tous les dommages et intérêts envers l'acquéreur.

Si le vendeur n'avait pas connaissance du vice et a stipulé qu'il ne sera tenu à aucune garantie au titre des vices cachés, il n'est tenu par aucune obligation de restitution du prix ou de dommages et intérêts.

Article 545 Destruction du bien

Si le bien vicié a été détruit ou disparaît par suite de sa mauvaise qualité, la perte est imputable au vendeur, qui sera tenu envers l'acquéreur à la restitution du prix et le cas échéant, au paiement de dommages-intérêts.

Si la destruction ou disparition du bien vicié est fortuite, l'acquéreur assume seul la perte.

Article 546 Prescription

L'action résultant des vices cachés est prescrite après un délai de deux (2) ans à compter de la découverte du vice.

Chapitre 4 : Garantie d'éviction

Article 547 Application de la garantie d'éviction au commerce électronique

Toute personne exerçant une activité de commerce électronique en République de Djibouti ou à destination de personnes situées sur le territoire de la République de Djibouti garantit l'acquéreur de l'éviction qu'il souffre dans la totalité ou partie du bien vendu, ou des charges prétendues sur ce bien, et non déclarées lors de la vente.

La garantie d'éviction s'applique aux contrats portant sur la vente de biens mobiliers ou immobiliers.

Article 548 Contrats conclus entre professionnels

Dans le cadre de contrats conclus entre professionnels, les parties peuvent, par des dispositions particulières, aménager les effets et/ou les obligations liées à la garantie d'éviction. Elles peuvent également convenir que le vendeur ne sera soumis à aucune garantie.

Le vendeur reste tenu par la garantie d'éviction nonobstant toute clause contraire lorsque l'éviction résulte du fait personnel du vendeur.

Nonobstant d'éventuelles stipulations d'exclusion de garantie contre l'éviction, le vendeur, en cas d'éviction, est tenu à la restitution du prix, à moins que l'acquéreur n'ait connu lors de la vente le danger de l'éviction ou qu'il n'ait acquis le bien à ses risques et périls.

Article 549 Effets de la garantie d'éviction

Lorsque la garantie d'éviction a été promise, ou qu'il n'a rien été stipulé à ce sujet, si l'acquéreur est évincé, il a droit de demander au vendeur :

1. la restitution du prix ;

2. la restitution des fruits, lorsqu'il est obligé de les rendre au propriétaire qui l'évince ;

3. les frais faits sur la demande en garantie de l'acquéreur, et ceux faits par le demandeur originaire ;

4. des dommages-intérêts, ainsi que le remboursement des frais et loyaux coûts du contrat.

Si au moment de l'éviction le bien vendu se trouve diminué de valeur ou considérablement détérioré, soit par la négligence de l'acquéreur soit par des faits relevant de la force majeure, le vendeur reste tenu de restituer la totalité du prix.

Si en revanche l'acquéreur a tiré profit des dégradations faites par lui, le vendeur a le droit de retenir sur le prix une somme égale à ce profit.

Article 550 Mauvaise foi du vendeur

Si le vendeur a vendu de mauvaise foi le bien d'autrui, il est tenu de rembourser à l'acquéreur toutes les dépenses, même d'agrément, que celui-ci aura faites pour le bien.

Article 551 Application en cas d'éviction partielle

Si l'acquéreur n'est évincé que d'une partie du bien qui, relativement au tout, est d'une importance telle que l'acquéreur n'aurait pas acquis le bien dans son ensemble sans la partie dont il a été évincé, il peut demander la résolution de la vente.

Si la vente n'est pas résolue, la valeur de la partie du bien dont l'acquéreur se trouve évincé lui est remboursée suivant l'estimation à l'époque de l'éviction, et non proportionnellement au prix total de la vente, que la chose vendue ait augmenté ou diminué de valeur.

Article 552 Augmentation du prix

Si le bien vendu se trouve avoir augmenté de valeur au moment de l'éviction, même indépendamment du fait de l'acquéreur, le vendeur est tenu de lui payer ce qu'il vaut au-dessus du prix de la vente.

Article 553 Remboursement des réparations et améliorations

Le vendeur est tenu de rembourser à l'acquéreur, ou de faire rembourser par celui qui l'évince, toutes les réparations et améliorations utiles qu'il aura faites au bien.

Article 554 Prescription

La garantie d'éviction cesse lorsque l'acquéreur s'est laissé condamner par un jugement en dernier ressort, ou dont l'appel n'est plus recevable, sans avoir appelé le vendeur, si celui-ci prouve qu'il existait des moyens suffisants de faire rejeter la demande.

Livre Sixième : Cybersécurité

Titre 1 Des infractions liées aux technologies de l'information et de la communication

Chapitre 1 : Atteintes aux systèmes informatiques

Section 1 : Atteintes à la confidentialité des systèmes informatiques

Article 555 Accès frauduleux à des systèmes informatiques

Quiconque aura accédé ou tenté d'accéder frauduleusement à tout ou une partie d'un système informatique sera puni d'une peine d'emprisonnement maximum de trois (3) ans et d'une amende maximum de 10.000.000 DJF ou de l'une de ces deux peines seulement.

Article 556 Maintien d'un accès frauduleux à des systèmes informatiques

Quiconque se maintient ou tente de se maintenir à tout ou une partie d'un système informatique après s'y être introduit frauduleusement sera puni d'un emprisonnement de trois (3) ans et d'une amende maximum de 10.000.000 DJF ou de l'une de ces deux peines seulement.

Article 557 Sanctions

Les peines prévues aux Article 555 et Article 556 sont portées à une peine d'emprisonnement maximum de cinq (5) ans et une amende maximum de 25.000.000 DJF lorsque l'accès ou le maintien frauduleux à tout ou une partie d'un système informatique entraîne la suppression ou la modification de données contenues dans le système informatique.

Section 2 : Atteintes à l'intégrité des systèmes informatiques

Article 558 Introduction frauduleuse de données dans un système informatique

Quiconque aura introduit ou tenté d'introduire frauduleusement des données dans un système informatique, sera puni d'une peine d'emprisonnement maximum de cinq (5) ans et d'une amende maximum de 25.000.000 DJF ou de l'une de ces deux peines seulement.

Section 3 : Atteintes à la disponibilité des systèmes informatiques

Article 559 Atteintes au fonctionnement d'un système informatique

Quiconque aura troublé, altéré ou faussé ou aura tenté de troubler, d'altérer, ou de fausser le fonctionnement d'un système informatique sera puni d'une peine d'emprisonnement maximum de cinq (5) ans et d'une amende maximum de 25.000.000 DJF ou de l'une de ces deux peines seulement.

Chapitre 2 : Atteintes aux données informatisées

Section 1 : Atteintes générales aux données informatisées

Article 560 Interception de données informatisées

Quiconque aura intercepté ou tenté d'intercepter frauduleusement par des moyens techniques des données informatisées lors de leur transmission non publique à destination, en provenance ou à l'intérieur d'un système informatique, sera puni d'un emprisonnement maximum de cinq (5) ans et d'une amende maximum de 25.000.000 DJF ou de l'une de ces deux peines seulement.

Article 561 Endommagement de données informatisées

Quiconque aura endommagé ou tenté d'endommager, effacé ou tenté d'effacer, détérioré ou tenté de détériorer, altéré ou tenté d'altérer, modifié ou tenté de modifier frauduleusement des données informatisées, sera puni d'un emprisonnement maximum de cinq (5) ans et d'une amende maximum de 25.000.000 DJF ou de l'une de ces deux peines seulement.

Article 562 Production ou fabrication de données informatisées

Quiconque aura produit ou fabriqué un ensemble de données numérisées par l'introduction, l'altération, l'effacement ou la suppression frauduleuse de données informatisées stockées, traitées ou transmises par un système informatique, engendrant des données contrefaites, dans l'intention qu'elle soient prises en compte ou utilisées à des fins légales comme si elles étaient originales, sera puni d'un emprisonnement maximum de cinq (5) ans et d'une amende maximum de 25.000.000 DJF ou de l'une de ces deux peines seulement.

Article 563 Usage de données produites ou fabriquées

Est puni des mêmes peines celui qui, en connaissance de cause, aura fait usage ou tenté de faire usage des données obtenues dans les conditions prévues à l'Article 562 du présent chapitre.

Article 564 Obtention frauduleuse d'avantages

Quiconque aura obtenu frauduleusement, pour lui-même ou pour autrui, un avantage quelconque, par l'introduction, l'altération, l'effacement ou la suppression de données informatisées ou par toute forme d'atteinte au fonctionnement d'un système informatique, sera puni d'une peine d'emprisonnement maximum de cinq (5) ans et d'une amende maximum de 25.000.000 DJF ou de l'une de ces deux peines seulement.

Chapitre 3 : Des autres formes d'abus

Article 565 Abus relatifs aux matériels et logiciels informatiques

Quiconque aura produit, vendu, importé, détenu, diffusé, offert, cédé ou mis à disposition un équipement, un programme informatique, tout dispositif ayant pour unique fonction de permettre la commission d'une ou plusieurs des infractions prévues par les articles Article 559 à Article 564 ou un mot de passe, un code d'accès ou des données informatisées similaires permettant d'accéder à tout ou partie d'un système informatique, sera puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

Article 566 Participation à une association ou une entente

Quiconque aura participé à une association formée ou à une entente établie en vue de préparer ou de commettre une ou plusieurs des infractions prévues par la présente loi, sera puni d'une peine de réclusion criminelle de dix (10) ans et d'une amende maximum de 25.000.000 DJF.

Article 567 Utilisation abusive de données informatisées permettant d'identifier une personne physique ou morale

Quiconque aura obtenu ou utilisé une ou plusieurs données de toute nature permettant d'identifier une personne physique ou morale par le biais d'un système informatique en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération sera puni d'une peine d'emprisonnement maximum de cinq (5) ans et d'une amende maximum de 25.000.000 DJF.

Article 568 Fausses données d'identification

Quiconque possède, utilise, vend, offre, met à disposition, transmet en toute connaissance de cause de fausses données d'identification sera puni d'une peine d'emprisonnement maximum de cinq (5) ans et d'une amende maximum de 25.000.000 DJF.

Article 569 Réalisation de fausses données d'identification

Quiconque réalise ou tente de réaliser de fausses données d'identification sera puni d'une peine d'emprisonnement maximum de cinq (5) ans et d'une amende maximum de 25.000.000 DJF.

Article 570 Atteinte à l'intimité de la vie privée d'autrui

Est puni d'une peine d'emprisonnement maximum de cinq (5) ans et d'une amende maximum de 25.000.000 DJF le fait, au moyen d'un ou sur un réseau de communication électronique ou un système informatique, de volontairement porter atteinte à l'intimité de la vie privée d'autrui :

1. En captant, enregistrant ou transmettant, sans le consentement de leur auteur, des paroles prononcées à titre privé ou confidentiel ;

2. En fixant, enregistrant ou transmettant, sans le consentement de celle-ci, l'image d'une personne se trouvant dans un lieu privé.

Lorsque les actes mentionnés au présent article ont été accomplis au vu et au su des intéressés sans qu'ils s'y soient opposés, alors qu'ils étaient en mesure de le faire, le consentement de ceux-ci est présumé.

Article 571 Correspondances par voie électronique

Le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder, de détourner ou de divulguer des correspondances émises, transmises ou reçues par la voie électronique arrivées ou non à destination et adressées à des tiers, ou d'en prendre frauduleusement connaissance, est puni d'une peine d'emprisonnement maximum de cinq (5) ans et d'une amende maximum de 25.000.000 DJF.

Est puni des mêmes peines le fait de procéder à l'installation d'appareils de nature à permettre la réalisation de telles interceptions.

Article 572 Publication de fausses informations en ligne

Est puni d'une peine d'emprisonnement maximum de cinq (5) ans et d'une amende maximum de 25.000.000 DJF le fait de publier sur Internet, par quelque voie que ce soit, le montage réalisé avec les paroles ou l'image d'une personne sans son consentement, s'il n'apparaît pas à l'évidence qu'il s'agit d'un montage ou s'il n'en est pas expressément fait mention.

Article 573 Enquête judiciaire

Les autorités judiciaires légalement compétentes peuvent, dans le cadre de leurs attributions et afin de prévenir la commission d'un délit ou d'un crime, pour les

nécessités d'une enquête judiciaire, ou dans le cadre d'une délégation judiciaire, procéder aux opérations prévues par les Article 565 et Article 566.

Chapitre 4 : Infractions en matière de données à caractère personnel

Article 574 Procédés illicites d'envoi de messages électroniques non sollicités

Quiconque utilise des procédés illicites d'envoi de messages électroniques non sollicités sur la base de la collecte de données à caractère personnel, sera puni d'une peine d'emprisonnement maximum d'un (1) an et d'une amende maximum de 10.000.000 DJF.

Article 575 Utilisation frauduleuse d'éléments d'identification

Quiconque utilise les éléments d'identification d'une personne physique ou morale dans le but de tromper les destinataires d'un message électronique ou les usagers d'un site Internet en vue de les amener à communiquer des données à caractère personnel ou des informations confidentielles sera puni d'une peine d'emprisonnement maximum de cinq (5) ans et d'une amende maximum de 25.000.000 DJF.

Article 576 Détournement de fonds

Quiconque utilisera des données à caractère personnel ou des informations confidentielles communiquées dans le but de détourner des fonds publics ou privés sera puni d'une peine de réclusion criminelle de dix (10) ans et d'une amende maximum de 100.000.000 DJF.

Article 577 Traitement de données à caractère personnel sans information préalable

Quiconque aura procédé à un traitement de données à caractère personnel soit sans avoir préalablement informé individuellement les personnes de leur droit d'accès, de rectification ou d'opposition, de la nature des données transmises et des destinataires de celles-ci, soit malgré l'opposition de la personne concernée.

Chapitre 5 : Infractions aux biens

Article 578 Dispositions complétant certains codes

Les dispositions du présent chapitre viennent compléter les articles 2271-304 à 2271-308 du Code de commerce, et les articles 499 à 510, 516 à 521 et 527 à 540 du Code pénal.

Section 1 : Fraude aux cartes bancaires

Article 579 Utilisation frauduleuse de cartes bancaires

Est puni d'une peine d'emprisonnement maximum de sept (7) ans et d'une amende maximum d'un million (1.000.0000) de DJF le fait pour toute personne :

1. De contrefaire ou de falsifier une carte de paiement ou de retrait au moyen d'un ou sur un réseau de communication électronique ou un système informatique ;

2. De faire ou de tenter de faire usage, en connaissance de cause, d'une carte de paiement ou de retrait contrefaite ou falsifiée au moyen d'un ou sur un réseau de communication électronique ou un système informatique ;

3. D'accepter, en connaissance de cause, de recevoir un paiement au moyen d'une carte de paiement contrefaite ou falsifiée au moyen d'un ou sur un réseau de communication électronique ou un système informatique.

Article 580 Utilisation de matériels et programmes informatiques pour utilisation frauduleuse de cartes bancaires

Est puni d'une peine d'emprisonnement maximum de sept (7) ans et d'une amende maximum de1.400.000 DJF le fait, pour toute personne, de fabriquer, d'acquérir, de détenir, de céder, d'offrir ou de mettre à disposition des équipements, instruments, programmes informatiques ou toutes données conçus ou spécialement adaptés pour commettre les infractions prévues à l'Article 575.

Article 581 Confiscation de cartes de paiement contrefaites ou falsifiées

La confiscation, aux fins de destruction des cartes de paiement contrefaites ou falsifiées est obligatoire dans les cas prévus aux Article 579 et Article 580. Est également obligatoire la confiscation des matières, machines, appareils, instruments, programmes informatiques ou de toutes données qui ont servi ou étaient destinés à servir à la fabrication desdits objets, sauf lorsqu'ils ont été utilisés à l'insu du propriétaire.

Article 582 Interdiction des droits civiques, civils et de famille et d'exercer une activité professionnelle ou sociale

Dans tous les cas prévus auxArticle 579 et Article 580, le tribunal peut prononcer l'interdiction des droits civiques, civils et de famille ainsi que l'interdiction, pour une durée de cinq (5) ans au plus, d'exercer une activité professionnelle ou sociale.

Article 583 Répression de la tentative

La tentative des délits prévus aux Article 579 et Article 580 est punie des mêmes peines

Section 2 : Escroquerie

Article 584 Escroquerie en ligne

Est puni d'une peine d'emprisonnement maximum de **2 à 7** ans et d'une amende égale au quintuple de la valeur mise en cause sans qu'elle soit inférieure 700.000 DJF le fait, au moyen d'un ou sur un réseau de communication électronique ou un système informatique, de tromper une personne physique ou morale, soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manœuvres frauduleuses et de déterminer ainsi la personne physique ou morale, à son préjudice ou au préjudice de tiers, à remettre des fonds, des valeurs ou une chose quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge.

Article 585 Eléments aggravants

La peine prévue à l'Article 584 est portée à dix (10) ans de réclusion criminelle et à une amende égale au quintuple de la valeur mise en cause sans qu'elle soit inférieure à 17.500.000DJF lorsque l'escroquerie est réalisée par :

1. Un agent de l'autorité publique ou d'un service d'intérêt public ou par une personne qui prend indûment cette qualité ;

2. Par une personne qui fait appel au public en vue de l'émission de titres ou de la collecte de fonds à des fins d'entraide humanitaire ou sociale.

Article 586 Vente de titres d'accès

Est puni d'une amende maximum de 2.000.000 DJF le fait de vendre, d'offrir à la vente ou d'exposer en vue de la vente ou de la cession ou de fournir les moyens en vue de la vente ou de la cession au moyen d'un ou sur un réseau de communication électronique ou un système informatique, des titres d'accès à une manifestation sportive, culturelle ou commerciale ou à un spectacle vivant, de manière habituelle et sans l'autorisation du producteur ; de l'organisateur, ou du propriétaire des droits d'exploitation de cette manifestation ou de ce spectacle.

Section 3 : Abus de confiance

Article 587 Détournement d'une chose remise dans un but déterminé

Est puni d'une peine d'emprisonnement maximum d'1 à 5 ans et d'une amende maximum de 100.000 DJF à 1.000.000 DJF le fait pour une personne, au moyen d'un ou sur un réseau de communication électronique ou un système informatique de détourner, au préjudice d'autrui, une chose quelconque qui lui a été remise et qu'elle a acceptée à charge de la rendre, de la représenter ou d'en faire un usage déterminé.

Article 588 Elément aggravants

La peine prévue à l'Article 587 est doublée lorsque l'abus de confiance est réalisé :

1. Par une personne qui fait appel au public afin d'obtenir la remise de fonds ou de valeurs, soit pour son propre compte, soit pout comme dirigeant ou préposé de droit ou de fait d'une entreprise industrielle ou commerciale ;

2. Par un mandataire de justice ou par un officier public ou ministériel, soit dans l'exercice de ses fonctions soit en raison de sa qualité ;

3. Par toute autre personne qui, de manière habituelle, se livre ou prête son concours, même à titre accessoire, à des opérations portant sur les biens des tiers pour le compte desquels elle recouvre des fonds ou des valeurs.

Section 4 : Recel

Article 589 Utilisation d'un produit d'une infraction

Est puni d'une peine d'emprisonnement maximum de 5 à 10 ans et d'une amende maximum de 3.500.000 DJF à 7.000.000DJF le fait, par une personne, au préjudice des droits d'autrui, de détenir, d'utiliser ou de transmettre une chose en sachant que celle-ci provient d'une infraction au moyen d'un ou sur un réseau de communication électronique ou un système informatique. Constitue également un recel le fait par une personne, dans les mêmes conditions, de faire office d'intermédiaire afin de transmettre la chose.

Article 590 Eléments aggravants

Les peines sont portées à dix (10) ans de réclusion criminelle et à 17.500.000DJF d'amende lorsque la personne se livre au recel au moyen d'un ou sur un réseau de communication électronique ou un système informatique, de manière habituelle ou lorsqu'elle s'y livre à l'occasion de l'exercice de sa profession.

Section 5 : Extorsion

Article 591 Extorsion au moyen d'un ou sur un réseau de communications électroniques ou un système informatique

Est puni d'une peine d'emprisonnement maximum d'1 an à 5 ans et d'une amende maximum de 350.000 DJF à 3.500.000DJF le fait d'extorquer par violence, menace de violence ou contrainte, soit une signature, un engagement ou une renonciation, soit la révélation d'un secret, soit la remise de fonds, de valeurs ou d'une chose quelconque au moyen d'un ou sur un réseau de communication électronique ou un système informatique.

Article 592 Extorsion en bande organisée

L'extorsion en bande organisée est punie de dix (10) ans de réclusion criminelle et d'une amende maximum de dix (10) millions de DJF.

Section 6 : Chantage

Article 593 Chantage sur un réseau de communication électronique ou sur un système informatique

Quiconque extorque, en menaçant de révéler ou d'imputer des faits de nature à porter atteinte à l'honneur ou à la considération, soit une signature, un engagement ou une renonciation, soit la révélation d'un secret, soit la remise de fonds, de valeurs ou d'une chose quelconque au moyen d'un ou sur un réseau de communication électronique ou un système informatique, sera puni d'une peine d'emprisonnement maximum de 6 ans et d'une amende maximum de 3.500.000DJF.

Section 7 : Blanchiment de capitaux

Article 594 Blanchiment de capitaux au moyen d'un ou sur un réseau de communication électronique

Les dispositions de la loi n° 112/AN/11/6ème L complétant la loi n° 196/AN/02/4ème L sur le blanchiment, la confiscation et la coopération internationale en matière de produit du crime seront aussi d'application en cas de blanchiment de capitaux au moyen d'un ou sur un réseau de communication électronique ou un système informatique.

Chapitre 6 : Infraction se rapportant au contenu

Section 1 : Protection de l'enfance

Article 595 Pornographie infantile via un système informatique

Quiconque aura produit, enregistré, offert, mis à disposition, diffusé, transmis une image ou une représentation présentant un caractère de pornographie infantile par le biais d'un système informatique, sera puni d'une peine de réclusion criminelle de 2 à 7 ans et d'une amende maximum de 14.000.000 DJF à 70.000.000 DJF.

Article 596 Import et export d'image ou représentation de pornographie infantile

Quiconque se sera procuré ou aura procuré à autrui, importé ou fait importer, exporté ou fait exporter une image ou une représentation présentant un caractère de pornographie infantile par le biais d'un système informatique, sera puni d'une peine de réclusion criminelle de 6 mois à 5 ans et d'une amende maximum de 35.000.000 DJF à 350.000.000 DJF.

Article 597 Possession d'image ou de représentation de pornographie infantile et accès facilité

Sera puni des mêmes peines, celui qui possède une image ou une représentation présentant un caractère de pornographie infantile dans un système informatique ou dans un moyen quelconque de stockage de données informatisées.

Sera puni des mêmes peines, quiconque aura facilité l'accès à des images, des documents, du son ou une représentation présentant un caractère de pornographie à un mineur.

Article 598 Consultation habituelle de pornographie infantile en ligne

Le fait de consulter habituellement un service de communication au public en ligne mettant à disposition une image ou représentation présentant un caractère de pornographie infantile est puni d'une peine de réclusion criminelle de 10 ans et d'une amende maximum de 17.500.000 DJF.

Article 599 Fabrication, transport et diffusion de certains messages

Quiconque fabrique, transporte, diffuse au moyen d'un ou sur un réseau de communication électronique ou un système informatique, un message à caractère violent, pornographique ou de nature à porter gravement atteinte à la dignité humaine ou à inciter des mineurs à se livrer à des jeux les mettant physiquement en danger, soit fait commerce d'un tel message au moyen ou sur un réseau de communication électronique ou un système informatique, sera puni d'une amende maximum de 350.000 DJF à 3.500.000 DJF lorsque ce message est susceptible d'être vu ou perçu par un mineur.

Article 600 Promotion, encouragement et facilitation à la réalisation de certaines infractions

Quiconque promeut, encourage ou facilite les comportements incriminés aux Article 598 et Article 599 au moyen d'un ou sur un réseau de communication électronique ou un système informatique est puni d'une peine de réclusion criminelle de dix (10) ans et d'une amende maximum de 350.000 DJF à 7.000.000 DJF.

Article 601 Corruption de mineur au moyen d'un ou sur un réseau de communication électronique ou sur un système informatique

Quiconque favorisera ou tentera de favoriser la corruption d'un mineur au moyen d'un ou sur un réseau de communication électronique ou un système informatique sera puni d'une peine de réclusion criminelle de 10 ans et d'une amende maximum de 17.500.000 DJF.

Les peines sont portées au double lorsque les faits à l'encontre d'un mineur de moins de quinze (15) ans.

Article 602 Propositions sexuelles à mineur de moins de quinze ans sur un réseau de communication électronique ou un système informatique

Quiconque fera des propositions sexuelles à un mineur de moins de quinze (15) ans ou à une personne se présentant comme telle au moyen d'un ou sur un réseau de communication électronique ou un système informatique sera puni d'une peine de réclusion criminelle de 2 à 7 ans et d'une amende de 14.000.000 DJF à 70.000.000 DJF.

Ces peines sont portées à 10 à 20 ans de réclusion criminelle et 70.000.000 DJF à 350.000.000 DJF d'amende lorsque les propositions ont été suivies d'une rencontre.

Article 603 Commission des infractions de la présente section en bande organisée

Les infractions prévues à la présente section, lorsqu'elles ont été commises en bande organisée, seront punies d'une peine de réclusion criminelle de 4 à 14 ans et d'une amende maximum de 140.000.000 DJF à 700.000.000 DJF.

Section 2 : Infractions sexuelles et prostitution sur internet

Article 604 Viol à la suite d'une mise en contact sur un réseau de communication électronique ou un système informatique

Le viol est puni d'une peine de réclusion criminelle de 20 ans et d'une amende maximum de 35.000.000DJF lorsque la victime a été mise en contact avec l'auteur des faits au moyen d'un ou sur un réseau de communication électronique ou un système informatique.

Est puni des mêmes peines le fait d'enregistrer sciemment, par quelque moyen que ce soit, sur tout support que ce soit, des images relatives à la commission d'un viol.

Le fait de diffuser l'enregistrement de telles images est puni d'une peine d'emprisonnement maximum de cinq (5) ans et d'une amende maximum de 1.000.000 DJF.

Article 605 Agressions sexuelles à la suite d'une mise en contact sur un réseau de communications électroniques ou un système informatique

Les agressions sexuelles prévues à la section III du code pénal de Djibouti, autres que le viol, sont punies d'une peine d'emprisonnement maximum de 10 ans et d'une amende maximum de 17.500.000 DJF lorsque la victime a été mise en contact avec l'auteur des faits au moyen d'un ou sur un réseau de communication électronique ou un système informatique.

Article 606 Prostitution de mineurs sur un réseau de communication électronique ou un système informatique

Le fait de solliciter, d'accepter ou d'obtenir, en échange d'une rémunération ou d'une promesse de rémunération, des relations de nature sexuelle de la part d'un mineur qui se livre à la prostitution, y compris de façon occasionnelle, est puni de d'une peine d'emprisonnement de 20 ans et d'une amende maximum de 35.000.000DJF lorsque la personne a été mise en contact avec l'auteur des faits au moyen d'un ou sur un réseau de communication électronique ou un système informatique.

Article 607 Prostitution de personnes vulnérables sur un réseau de communication électronique ou un système informatique

Est puni des mêmes peines le fait de solliciter, d'accepter ou d'obtenir, en échange d'une rémunération ou d'une promesse de rémunération, des relations sexuelles de la part d'une personne qui se livre à la prostitution, y compris de façon occasionnelle, lorsque cette personne présente une particulière vulnérabilité, apparente ou connue de son auteur, due à une maladie, à une infirmité, à une déficience physique ou psychique ou à un état de grossesse.

Section 3 : Diffamation, injure et dénonciation calomnieuse

Article 608 Diffamation sur un réseau de communication électronique ou sur un système informatique

Toute allégation ou imputation d'un fait qui porte atteinte à l'honneur ou à la considération de la personne auquel le fait est imputé au moyen d'un ou sur un réseau de communication électronique ou un système informatique est une diffamation.

La publication directe ou par voie de reproduction de cette allégation ou de cette imputation au moyen d'un ou sur un réseau de communication électronique ou un système informatique est punissable même si elle est faite sous forme dubitative ou si elle vise une personne non expressément nommée, mais dont l'identification est rendue possible.

Article 609 Définition d'injure

Toute expression outrageante, termes de mépris ou invective exprimée à l'égard d'une personne ou d'un corps, même non expressément nommé mais identifiable, au moyen d'un ou sur un réseau de communication électronique ou un système informatique est une injure.

Article 610 Sanction de la diffamation et de l'injure envers les personnes exerçant des fonctions publiques

La diffamation et l'injure commise au moyen d'un ou sur un réseau de communication électronique ou un système informatique envers les personnes exerçant des fonctions publiques, sera punie d'une amende maximum de 700.000 DJF à 7.000.000 DJF.

Article 611 Sanction de la diffamation et de l'injure envers des particuliers ou groupes de particuliers

La diffamation et l'injure commises envers les particuliers au moyen d'un ou sur un réseau de communication électronique ou un système informatique sera punie d'une amende maximum de 700.000 DJF à 7.000.000 DJF.

La diffamation et l'injure commises par les mêmes moyens envers une personne ou un groupe de personnes à raison de leur origine ou de leur appartenance ou de leur non-appartenance à une ethnie, une nation, une race ou une religion déterminée ou à raison de leur sexe, sera punie d'une peine d'emprisonnement maximum de 6 mois à 7 ans et d'une amende maximum de 7.000.000 DJF.

Article 612 Dénonciation calomnieuse

La dénonciation, effectuée au moyen d'un ou sur un réseau de communication électronique ou un système informatique et dirigée contre une personne déterminée, d'un fait qui est de nature à entraîner des sanctions et que l'on sait totalement ou partiellement inexact, lorsqu'elle est adressée soit à un officier de justice ou de police, soit à une autorité ayant le pouvoir d'y donner suite ou de saisir l'autorité compétente, soit aux supérieurs hiérarchiques ou à l'employeur de la personne dénoncée, est punie d'une peine d'emprisonnement maximum de 5 ans et d'une amende maximum de 700.000 DJF.

Lorsque le fait dénoncé a donné lieu à des poursuites pénales, il ne peut être statué sur les poursuites exercées contre l'auteur de la dénonciation qu'après la décision mettant définitivement fin à la procédure concernant le fait dénoncé.

Section 4 : Infractions commises en raison de la couleur, l'appartenance à une race, a une origine nationale ou ethnique, a une religion ou à un handicap

Article 613 Messages et représentations racistes, xénophobes, discriminatoires en ligne

Quiconque aura créé, téléchargé, diffusé ou mis à disposition sous quelque forme que ce soit des écrits, messages, photos, dessins ou toute autre représentation d'idées ou de théories, de nature raciste ou xénophobe, ou discriminatoire en raison notamment de l'appartenance à la religion, ou à un handicap par le biais d'un système informatique sera

puni d'une peine d'emprisonnement maximum de 6 mois à 7 ans et d'une amende maximum de 700.000 DJF à 7.000.000 DJF.

Article 614 Menaces en ligne

La menace commise par le biais d'un système informatique, de commettre une infraction pénale, envers une personne en raison de son appartenance à un groupe qui se caractérise par l'appartenance à une race, à une couleur, à une origine nationale ou ethnique, à la religion, ou à un handicap dans la mesure où cette appartenance sert de prétexte à l'un ou l'autre de ces éléments, sera puni d'une peine de réclusion criminelle de dix (10) ans et d'une amende maximum de 700.000 DJF à 7.000.000 DJF.

Article 615 Provocation à la discrimination, la haine ou la violence en ligne

Quiconque aura provoqué à la discrimination, à la haine ou à la violence à l'égard d'une personne ou d'un groupe de personnes à raison de l'appartenance à une race, à une couleur, à une origine nationale ou ethnique, à la religion, ou à un handicap au moyen d'un ou sur un réseau de communication électronique ou un système informatique, sera puni de dix (10) ans de réclusion criminelle et d'une amende de 3.500.000 DJF ou de l'une de ces deux peines seulement.

Section 5 : Autres atteintes portant sur le contenu

Article 616 Enregistrement et diffusion en ligne d'images relatives à la commission d'infractions

Est constitutif d'un acte de complicité des atteintes volontaires à l'intégrité de la personne le fait d'enregistrer sciemment, par quelque moyen que ce soit, sur tout support que ce soit, des images relatives à la commission d'infractions.

Le fait de diffuser l'enregistrement de telles images est puni d'une peine d'emprisonnement maximum de 5 ans et d'une amende maximum de 17.500.000DJF.

Le présent article n'est pas applicable lorsque l'enregistrement ou la diffusion résulte de l'exercice normal d'une profession ayant pour objet d'informer le public ou est réalisé afin de servir de preuve en justice.

Article 617 Appel à un mouvement insurrectionnel en ligne

Est punie d'une peine d'emprisonnement maximum de 12 mois et d'une amende maximum de 1.000.000DJF l'appel à un mouvement insurrectionnel au moyen d'un ou sur un réseau de communication électronique ou un système informatique.

Constitue un mouvement insurrectionnel toute violence collective de nature à mettre en péril les institutions de la République ou à porter atteinte à l'intégrité du territoire national.

Article 618 Incitation en ligne à la commission d'infractions

Seront punis comme complices d'une action qualifiée de crime ou de délit ceux qui au moyen d'un ou sur un réseau de communication électronique ou un système informatique auront directement provoqué l'auteur ou les auteurs à commettre ladite action, si la provocation a été suivie d'effet.

Article 619 Incitation en ligne à la commission de certaines infractions

Seront punis de dix (10) ans de réclusion criminelle et d'une amende maximum de 3.500.000 DJF d'amende ceux qui, par l'un des moyens énoncés à l'article précédent, auront directement provoqué, dans le cas où cette provocation n'aurait pas été suivie d'effet, à commettre l'une des infractions suivantes au moyen d'un ou sur un réseau de communication électronique ou un système informatique :

1. Les atteintes à la vie de la personne, les atteintes à l'intégrité physique de la personne et les agressions sexuelles, définies par le Code pénal ;

2. Les vols, les extorsions dangereuses pour les personnes, définis par le Code pénal.

Article 620 Négationnisme, justification et apologie de crimes de guerre et de crimes contre l'humanité

Seront punis d'une peine de réclusion criminelle de dix (10) ans et d'une amende maximum de 700.000 DJF à 7.000.000 DJF ceux qui, au moyen d'un ou sur un réseau de communication électronique ou un système informatique auront nié, justifié ou fait l'apologie des crimes de guerre et crimes contre l'humanité.

Article 621 Provocation au suicide en ligne

Le fait de provoquer au moyen d'un ou sur un réseau de communication électronique ou un système informatique au suicide d'autrui est puni d'une peine d'emprisonnement maximum de 3 ans et d'une amende maximum de 1.000.000 DJF lorsque la provocation a été suivie du suicide ou d'une tentative de suicide.

Article 622 Provocation à certains actes de terrorisme en ligne

Quiconque aura, au moyen d'un ou sur un réseau de communication électronique ou un système informatique, provoqué directement aux actes de terrorisme prévus par le Code pénal, la loi n° 111/AN/11/6èmeL relative à la lutte contre le terrorisme et autres, ou toute autre loi ultérieure en matière de terrorisme ou qui en aura fait l'apologie sera puni de dix (10) ans de réclusion criminelle et d'une amende maximum de 17.500.000 DJF.

Article 623 Diffusion en ligne de procédés permettant la fabrication d'engins de destruction

Le fait de diffuser, au moyen d'un ou sur un réseau de communication électronique ou un système informatique, sauf à destination des professionnels, des procédés permettant la fabrication d'engins de destruction élaborés à partir de poudre ou de substances explosives, de matières nucléaires, biologiques ou chimiques, ou à partir de tout autre produit destiné à l'usage domestique, industriel ou agricole, est puni de dix (10) ans de réclusion criminelle et d'une amende maximum de 17.500.000 DJF.

Article 624 Condamnation accessoire

En cas de condamnation, le tribunal pourra prononcer la confiscation des matériels équipements, instruments, programmes informatiques ou tous dispositifs ou données appartenant au condamné et ayant servi à commettre les infractions prévues à la présente Section.

Chapitre 7 : Atteinte aux droits de la propriété intellectuelle et industrielle

Article 625 Dispositions complétant certaines lois

Les dispositions du présent chapitre viennent compléter les dispositions de la loi n° 50/AN/09/6ème L portant protection de la propriété industrielle et de la loi n° 154/AN/06 du 23 juillet 2006 relative à la protection du droit d'auteur et du droit voisin.

Section 1 : Atteinte aux droits de propriété intellectuelle

Article 626 Atteinte en ligne à certains droits des propriétaires

Toute atteinte portée au moyen d'un ou sur un réseau de communication électronique ou un système informatique aux droits du propriétaire d'un brevet, d'un certificat d'addition, d'un certificat de schéma de configuration (topographie) de circuits intégrés, aux dessins et modèles industriels ou d'un certificat d'enregistrement de marque de produits ou de services tels qu'ils sont respectivement définis aux articles 53, 54, 98, 122,123, 153 et 154 de la loi n° 50/AN/09/6eme L du 19 juillet 2009 portant protection de la propriété intellectuelle constitue une contrefaçon.

Article 627 Usage non autorisée de marque et utilisation frauduleuse de marque en ligne

Sont punis d'une peine d'emprisonnement maximum de 2 ans et d'une amende de 350.000 DJF à 7.000.000 DJF, lorsqu'ils sont commis au moyen d'un ou sur un réseau de communication électronique ou un système informatique :

1. L'usage d'une marque sans l'autorisation de son propriétaire même avec l'adjonction des mots tels que « formule, « façon », système, « recette », « imitation », « genre » ou de tout autre indication similaire propre à tromper l'acheteur ;

2. La mise en vente de produits et services revêtus d'une marque qu'ils savaient revêtus d'une marque frauduleusement imitée.

Article 628 Utilisation d'indications et de données fausses ou fallacieuses en ligne

Sont punis d'une peine d'emprisonnement maximum de 2] ans et d'une amende maximum de 350.000 DJF à 7.000.000 DJF, lorsqu'ils sont commis au moyen d'un ou sur un réseau de communication électronique ou un système informatique :

1. L'utilisation directe ou indirecte d'une indication fausse ou fallacieuse concernant la provenance d'un produit ou d'un service, ou l'identité du producteur, fabricant ou commerçant;

2. L'utilisation directe ou indirecte d'une indication géographique ou d'une appellation d'origine fausse ou fallacieuse, ou l'imitation d'une indication géographique ou d'une appellation d'origine, même si l'origine véritable du produit est indiquée ou si l'appellation est employée en traduction ou accompagnée d'expressions telles que « genre », « façon », « imitation » ou similaires.

Article 629 Reproduction, représentation et mise à disposition du public un dessin ou un modèle protégé en ligne

Constitue une atteinte à la propriété intellectuelle punie d'une peine d'emprisonnement maximum de 2 ans et d'une amende maximum de 350.000 DJF à 7.000.000 DJF, le fait, sans autorisation de l'auteur ou de ses ayants droits de reproduire, représenter ou de mettre à la disposition du public un dessin ou un modèle protégé par le droit d'auteur ou un droit voisin au moyen d'un ou sur un réseau de communication électronique ou un système informatique.

Article 630 Vente ou mise à disposition du public un bien ou un produit protégé en ligne

Constitue une atteinte à la propriété intellectuelle punie d'une peine d'emprisonnement maximum de 2 ans et d'une amende maximum de 350.000 DJF à 7.000.000 DJF le fait, en toute connaissance de cause, sans droit, de vendre ou de mettre à disposition du public par reproduction ou par représentation un bien ou un produit protégé par un brevet d'invention au moyen d'un ou sur un réseau de communication électronique ou un système informatique.

Article 631 Vente ou mise à disposition du public des schémas de configuration de circuits intégrés en ligne

Constitue une atteinte à la propriété intellectuelle punie d'une peine d'emprisonnement maximum de 2 ans et d'une amende maximum de 350.000 DJF à 7.000.000 DJF le fait, en toute connaissance de cause, sans droit, de vendre ou de mettre à disposition du public par reproduction ou par représentation un schéma de configuration (topographie) de circuits intégrés au moyen d'un ou sur un réseau de communication électronique ou un système informatique.

Section 2 : L'échange illicite et téléchargement sur internet

Article 632 Fixation, reproduction, communication et mise à disposition du public de programmes divers

Est punie d'une peine d'emprisonnement maximum de 3 ans et d'une amende maximum de 1.000.000 DJF toute fixation, reproduction, communication ou mise à disposition du public, à titre onéreux ou gratuit, ou toute télédiffusion d'une prestation, d'un phonogramme, d'un vidéogramme ou d'un programme, réalisée sans l'autorisation, lorsqu'elle est exigée, de l'artiste-interprète, du producteur de phonogrammes ou de vidéogrammes ou de l'entreprise de communication audiovisuelle.

Sont punis des mêmes peines l'importation, l'exportation, le transbordement ou la détention aux fins précitées de phonogrammes ou de vidéogrammes réalisée sans l'autorisation du producteur ou de l'artiste-interprète, lorsqu'elle est exigée.

Est puni de la peine d'amende prévue au premier alinéa le défaut de versement de la rémunération due à l'auteur, à l'artiste-interprète ou au producteur de phonogrammes ou de vidéogrammes au titre de la copie privée ou de la communication publique ainsi que de la télédiffusion des phonogrammes.

Lorsque les délits prévus au présent article ont été commis en bande organisée, les peines sont portées au double.

Article 633 Logiciel donnant frauduleusement accès à des œuvres protégées

Est puni d'une peine d'emprisonnement maximum de 3 ans et d'une amende maximum de 2.000.000 DJF le fait :

1. D'éditer, de mettre à la disposition du public ou de communiquer au public, sciemment et sous quelque forme que ce soit, un logiciel manifestement destiné à la mise à disposition du public non autorisée d'œuvres protégées.

2. D'inciter sciemment, y compris à travers une annonce publicitaire, à l'usage d'un logiciel mentionné au 1), au moyen d'un ou sur un réseau de communication électronique ou un système informatique.

Article 634 Pouvoir d'injonction du Tribunal

En présence d'une atteinte à un droit d'auteur ou à un droit voisin occasionnée par le contenu d'un service de communication au public en ligne, le Tribunal de Première Instance, peut ordonner à la demande des titulaires de droits sur les œuvres et objets protégés, de leurs ayants droit, toutes mesures propres à prévenir ou à faire cesser une telle atteinte à un droit d'auteur ou un droit voisin, à l'encontre de toute personne susceptible de contribuer à y remédier.

Article 635 Responsabilité de la personne titulaire de l'accès à des services de communication au public en ligne

La personne titulaire de l'accès à des services de communication au public en ligne a l'obligation de veiller à ce que cet accès ne fasse pas l'objet d'une utilisation à des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'œuvres ou d'objets protégés par un droit d'auteur ou par un droit voisin sans l'autorisation des titulaires des droits lorsqu'elle est requise.

Le manquement de la personne titulaire de l'accès à l'obligation définie au premier alinéa n'a pas pour effet d'engager la responsabilité pénale de l'intéressé, sous réservedes Article 632 et Article 633.

Article 636 Pouvoirs du Bureau de droit d'auteur et droit voisin

En cas d'infraction définie à l'Article 635, le Bureau de droit d'auteur et droit voisin peut envoyer à l'abonné, sous son timbre et pour son compte, par la voie électronique et par l'intermédiaire de la personne dont l'activité est d'offrir un accès à des services de communication au public en ligne ayant conclu un contrat avec l'abonné, une recommandation lui rappelant les dispositions de l'Article 635, lui enjoignant de respecter l'obligation qu'elles définissent et l'avertissant des sanctions encourues. Cette recommandation contient également une information de l'abonné sur l'offre légale de contenus culturels en ligne, sur l'existence de moyens de sécurisation permettant de prévenir les manquements à l'obligation définie à l'Article 635, ainsi que sur les dangers pour le renouvellement de la création artistique et pour l'économie du secteur culturel des pratiques ne respectant pas le droit d'auteur et les droits voisins.

En cas de renouvellement, dans un délai de six (6) mois à compter de l'envoi de la recommandation visée au premier alinéa, de faits susceptibles de constituer un manquement à l'obligation définie à l'Article 635, le Bureau de droit d'auteur et droit voisin peut adresser une nouvelle recommandation comportant les mêmes informations que la précédente par la voie électronique dans les conditions prévues au premier alinéa.

Elle doit assortir cette recommandation d'une lettre remise contre signature ou de tout autre moyen propre à établir la preuve de la date de présentation de cette recommandation.

Les recommandations adressées sur le fondement du présent article mentionnent la date et l'heure auxquelles les faits susceptibles de constituer un manquement à l'obligation définie à l'Article 635 ont été constatés. En revanche, elles ne divulguent pas le contenu des œuvres ou objets protégés concernés par ce manquement. Elles indiquent les coordonnées téléphoniques, postales et électroniques où leur destinataire peut adresser, s'il le souhaite, des observations au Bureau de droit d'auteur et droit voisin et obtenir, s'il en formule la demande expresse, des précisions sur le contenu des œuvres ou objets protégés concernés par le manquement qui lui est reproché.

Article 637 Peine complémentaire de suspension de l'accès

Lorsque l'infraction est commise au moyen d'un service de communication au public en ligne, les personnes coupables des infractions de contrefaçons peuvent en outre être condamnées à la peine complémentaire de suspension de l'accès à un service de communication au public en ligne pour une durée maximale d'un (1) an, assortie de l'interdiction de souscrire pendant la même période un autre contrat portant sur un service de même nature auprès de tout opérateur.

Lorsque ce service est acheté selon des offres commerciales composites incluant d'autres types de services, tels que services de téléphonie ou de télévision, les décisions de suspension ne s'appliquent pas à ces services.

La suspension de l'accès n'affecte pas, par elle-même, le versement du prix de l'abonnement au fournisseur du service.

Les frais d'une éventuelle résiliation de l'abonnement au cours de la période de suspension sont supportés par l'abonné.

Lorsque la décision est exécutoire, la peine complémentaire prévue au présent article est portée à la connaissance du Bureau de droit d'auteur et droit voisin qui la notifie à la personne dont l'activité est d'offrir un accès à des services de communication au public en ligne afin qu'elle mette en œuvre, dans un délai de quinze (15) jours au plus à compter de la notification, la suspension à l'égard de l'abonné concerné.

Le fait, pour la personne dont l'activité est d'offrir un accès à des services de communication au public en ligne, de ne pas mettre en œuvre la peine de suspension qui lui a été notifiée est puni d'une amende maximale de 350.000 DJF à 7.000.000 DJF.

Article 638 Sécurisation insuffisante de l'accès à Internet

La peine complémentaire définie à l'Article 637 peut être prononcée selon les mêmes modalités, en cas de négligence caractérisée définie à l'Article 639, à l'encontre du

titulaire de l'accès à un service de communication au public en ligne auquel le Bureau de droit d'auteur et droit voisin a préalablement adressé, par voie d'une lettre remise contre signature ou de tout autre moyen propre à établir la preuve de la date de présentation, une recommandation l'invitant à mettre en œuvre un moyen de sécurisation de son accès à Internet.

La négligence caractérisée s'apprécie sur la base des faits commis au plus tard un (1) an après la présentation de la recommandation mentionnée à l'alinéa précédent.

Dans ce cas, la durée maximale de la suspension est d'un (1) mois.

Le fait pour la personne condamnée à la peine complémentaire prévue par le présent article de ne pas respecter l'interdiction de souscrire un autre contrat d'abonnement à un service de communication au public en ligne pendant la durée de la suspension est puni d'une amende maximum de 450.000DJF.

Article 639 Négligence caractérisée

Constitue une négligence caractérisée le fait, sans motif légitime, pour la personne titulaire d'un accès à des services de communication au public en ligne :

1. soit de ne pas avoir mis en place un moyen de sécurisation de cet accès,

2. soit d'avoir manqué de diligence dans la mise en œuvre de ce moyen.

Les dispositions du premier alinéa ne sont applicables que lorsque se trouvent réunies les deux conditions suivantes :

1. Lorsque le titulaire de l'accès s'est vu recommander par le Bureau de droit d'auteur et droit voisin de mettre en œuvre un moyen de sécurisation de son accès permettant de prévenir le renouvellement d'une utilisation de celui-ci à des fins de reproduction, de représentation ou de mise à disposition ou de communication au public d'œuvres ou d'objets protégés par un droit d'auteur ou par un droit voisin sans l'autorisation des titulaires des droits,

2. Dans l'année suivant la présentation de cette recommandation, cet accès est à nouveau utilisé aux fins mentionnées au 1) du présent second alinéa.

Chapitre 8 : Autres infractions

Section 1 : Infractions relatives aux jeux en ligne

Article 640 Interdiction des jeux d'argent et de hasard sauf autorisation

Les jeux d'argent et de hasard de toute espèce organisée au moyen d'un ou sur un réseau de communication électronique ou un système informatique sont prohibés, sauf autorisation d'une autorité légalement compétente.

La République de Djibouti est en charge de publier un décret pris en Conseil des ministres définissant les conditions et modalités d'attribution d'une telle autorisation.

Cette interdiction recouvre les jeux dont le fonctionnement repose sur les connaissances du joueur.

Le sacrifice financier est établi dans les cas où l'organisateur exige une avance financière de la part des participants, même si le règlement du jeu prévoit la possibilité d'obtenir un remboursement ultérieur.

Les conditions et modalités d'attributions de ces jeux sont précisées sur proposition du ministère en charge de l'économie numérique par décret pris en conseil des ministres

Article 641 Cas des loteries sur Internet d'objets mobiliers dans un but d'intérêt social, culturel ou sportif

Sont exemptées des dispositions de l'Article 640, les loteries sur Internet d'objets mobiliers exclusivement destinées à des actes de bienfaisance, à l'encouragement des arts ou au financement d'activités sportives à but non lucratif, lorsqu'elles ont été autorisées par le Ministre de l'Intérieur.

Article 642 Sanction de la violation de l'interdiction des jeux d'argent et de hasard

La violation des interdictions prévues à l'Article 640 concernant les jeux d'argent et de hasard sur Internet est punie d'une peine d'emprisonnement maximum de 3 ans et d'une amende maximum de 35.000.000 DJF. Ces peines maximums sont portées au double lorsque l'infraction est commise en bande organisée.

Article 643 Participation à un jeu d'argent ou de hasard non autorisé

Quiconque participe à un jeu d'argent et de hasard non autorisé organisé au moyen ou sur un réseau de communication électronique ou un système informatique sera puni d'une peine d'emprisonnement d'une durée maximale de 3 ans ou d'une amende maximum de 35.000.000 DJF.

Section 2 : Infractions relatives à la publicité sur internet

Article 644 Propagande et publicité sur le tabac

Toute propagande ou publicité, directe ou indirecte, en faveur du tabac ou des produits du tabac réalisé au moyen d'un ou sur un réseau de communication électronique ou un système informatique est prohibée.

Est considérée comme propagande ou publicité indirecte toute propagande ou publicité en faveur d'un organisme, d'un service, d'une activité, d'un produit ou d'un article autre que le tabac ou un produit du tabac lorsque, par son graphisme, sa présentation, l'utilisation d'une marque, d'un emblème publicitaire ou de tout autre signe distinctif, elle rappelle le tabac ou un produit du tabac.

Article 645 Propagande ou publicité sur l'alcool

Toute propagande ou publicité, directe ou indirecte, en faveur de l'alcool réalisée au moyen d'un ou sur un réseau de communication électronique ou un système informatique est prohibée.

Est considérée comme propagande ou publicité indirecte toute propagande ou publicité en faveur d'un organisme, d'un service, d'une activité, d'un produit ou d'un article autre que l'alcool lorsque, par son graphisme, sa présentation, l'utilisation d'une marque, d'un emblème publicitaire ou de tout autre signe distinctif, elle rappelle l'alcool.

Article 646 Propagande ou publicité sur les jeux d'argent et de hasard

Toute propagande ou publicité, directe ou indirecte, en faveur d'un jeu d'argent et de hasard illicite réalisée au moyen d'un ou sur un réseau de communication électronique ou un système informatique est prohibée.

Est considérée comme propagande ou publicité indirecte toute propagande ou publicité en faveur d'un organisme, d'un service, d'une activité, d'un produit ou d'un article autre qu'un jeu de hasard et d'argent illicite, par son graphisme, sa présentation, l'utilisation d'une marque, d'un emblème publicitaire ou de tout autre signe distinctif, elle rappelle un jeu d'argent et de hasard illicite.

Article 647 Montant maximum de l'amende

Les infractions disposées aux articles Article 644 à Article 646 sont punies d'une amende maximum de 140.000.000 DJF. Le maximum de l'amende peut être porté à cinquante pour cent du montant des dépenses consacrées à l'opération illégale.

Section 3 : Traite des personnes et trafic illicite de migrants

Article 648 Renvoi à la loi spéciale

Sont punies des peines prévues par la loi N° 133/AN/16/7ème L les infractions relatives à la traite des personnes et au trafic illicite de migrants lorsqu'elles sont commises ou facilitées par des moyens informatiques.

Chapitre 9 : Responsabilité pénale des intermédiaires techniques

Section 1 : Des obligations communes aux fournisseurs d'accès et aux fournisseurs d'hébergement

Article 649 Absence d'obligation générale de surveillance des informations transmises et stockées

Les fournisseurs d'accès et d'hébergement ne sont pas soumis à une obligation générale de surveiller les informations qu'elles transmettent ou stockent, ni à une obligation générale de rechercher des faits ou des circonstances révélant des activités illicites.

Article 650 Pouvoirs en référé

Le Président du Tribunal de Première Instance peut prescrire en référé ou sur requête, à toute personne mentionnée à l'Article 649, toutes mesures propres à prévenir un dommage ou à faire cesser un dommage occasionné par le contenu d'un service de communication au public en ligne.

Article 651 Obligation de conservation

Les fournisseurs d'accès et d'hébergement détiennent et conservent pendant un (1) an les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont ils sont prestataires.

L'autorité judiciaire peut requérir communication auprès de ces personnes des données d'identification des destinataires de service dont elles sont prestataires.

Article 652 Mise en place d'un dispositif de signalement de contenus et activités illicites

Les fournisseurs d'accès et d'hébergement doivent mettre en place un dispositif facilement accessible et visible permettant à toute personne de porter à leur connaissance tout contenu et activité illicite.

Article 653 Obligation de notification aux autorités publiques

Les fournisseurs d'accès et d'hébergement ont l'obligation, d'une part, d'informer promptement les autorités publiques compétentes de tout contenu et activité illicite qui leur seraient signalées et qu'exerceraient les destinataires de leurs services, et, d'autre part, de rendre publics les moyens qu'ils consacrent à la lutte contre ces activités illicites.

Article 654 Sanctions

Est puni d'une peine d'emprisonnement maximum d'1 an et d'une amende maximum de 4.000.000 DJF le non-respect des obligations définies aux Articles Article 649 à Article 653.

Section 2 : Fournisseurs d'accès internet

Article 655 Absence de responsabilité civile et pénale de certaines personnes

Toute personne assurant une activité de transmission de contenus sur un réseau de communications électroniques ou de fourniture d'accès à un réseau de communications électroniques ne peut voir sa responsabilité civile ou pénale engagée à raison de ces contenus que dans les cas où soit elle est à l'origine de la demande de transmission litigieuse, soit elle sélectionne le destinataire de la transmission, soit elle sélectionne ou modifie les contenus faisant l'objet de la transmission.

Article 656 Moyens techniques de filtrage et obligation d'information

Les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne informent leurs abonnés de l'existence de moyens techniques permettant de restreindre l'accès à certains services ou de les sélectionner et leur proposent au moins un de ces moyens.

Est puni d'une peine maximum d'amende de 4.000.000 DJF quiconque ne respecte pas l'obligation d'information et de mise à disposition de moyens techniques de filtrage.

Section 3 : Fournisseurs d'hébergement

Article 657 Absence de responsabilité civile des fournisseurs d'hébergement pour les activités et informations stockées pour autrui

Les fournisseurs d'hébergement ne peuvent voir leur responsabilité civile engagée du fait des activités ou des informations stockées à la demande d'un destinataire de ces services s'ils n'avaient pas effectivement connaissance de leur caractère illicite ou de faits et circonstances faisant apparaître ce caractère ou si, dès le moment où ils en ont eu cette connaissance, ils ont agi promptement pour retirer ces données ou en rendre l'accès impossible.

La connaissance des faits litigieux est présumée acquise par les fournisseurs d'hébergement lorsqu'il leur est notifié les éléments suivants :

1. la date de la notification ;

2. si le notifiant est une personne physique : ses nom, prénoms, profession, domicile, nationalité, date et lieu de naissance ; si le requérant est une personne morale : sa forme, sa dénomination, son siège social et l'organe qui la représente légalement ;

3. le nom et domicile du destinataire ou, s'il s'agit d'une personne morale, sa dénomination et son siège social ;

4. la description des faits litigieux et leur localisation précise ;

5. les motifs pour lesquels le contenu doit être retiré, comprenant la mention des dispositions légales et des justifications de faits ;

6. la copie de la correspondance adressée à l'auteur ou à l'éditeur des informations ou activités litigieuses demandant leur interruption, leur retrait ou leur modification, ou la justification de ce que l'auteur ou l'éditeur n'a pu être contacté.

Article 658 Dénonciation erronée de contenus comme étant illicites

Le fait, pour toute personne physique ou morale, de présenter aux fournisseurs d'accès ou d'hébergement un contenu ou une activité comme étant illicite dans le but d'en obtenir le retrait ou d'en faire cesser la diffusion, alors qu'elle sait cette information inexacte, est puni d'une peine d'emprisonnement maximum d'1 an et d'une amende maximum de 3.500.000 DJF.

Article 659 Absence de responsabilité relative au stockage automatique

En cas de transmission sur un réseau de communication, des informations fournies par un destinataire du service, le fournisseur d'hébergement n'est pas responsable au titre du stockage automatique, intermédiaire et temporaire de cette information fait dans le seul but de rendre plus efficace la transmission ultérieure de l'information à la demande d'autres destinataires du service, à condition que le fournisseur d'hébergement :

1. ne modifie pas l'information ;

2. se conforme aux conditions d'accès à l'information ;

3. se conforme aux règles concernant la mise à jour de l'information, indiquées d'une manière largement reconnue et utilisées par les entreprises ;

4. n'entrave pas l'utilisation licite de la technologie, largement reconnue et utilisée par l'industrie, dans le but d'obtenir des données sur l'utilisation de l'information ; et

5. agisse promptement pour retirer l'information qu'il a stockée ou pour en rendre l'accès impossible dès qu'il a effectivement connaissance du fait que l'information à l'origine de la transmission a été retirée du réseau ou du fait que l'accès à l'information a été rendu impossible, ou du fait qu'un tribunal ou une autorité administrative a ordonné de retirer l'information ou d'en rendre l'accès impossible.

Section 4 : Fournisseurs de contenu

Article 660 Obligation d'information pesant sur les services de communication au public par voie électronique

Tout éditeur d'un service de communication au public par voie électronique a l'obligation de mettre à la disposition du public, dans un standard ouvert, des informations permettant de l'identifier. Les fournisseurs de contenu doivent mentionner sur leurs sites un certain nombre d'informations :

1. S'il s'agit de personnes physiques : leurs nom, prénoms, domicile et numéro de téléphone et, si elles sont assujetties aux formalités d'inscription au registre du commerce et des sociétés ou au répertoire des métiers, le numéro de leur inscription ;

2. S'il s'agit de personnes morales : leur dénomination ou leur raison sociale et leur siège social, leur numéro de téléphone et, s'il s'agit d'entreprises assujetties aux formalités d'inscription au registre du commerce et des sociétés ou au répertoire des métiers, le numéro de leur inscription, leur capital social, l'adresse de leur siège social.

Article 661 Mise à disposition d'informations sur l'hébergeur

Les personnes éditant à titre non professionnel un service de communication au public en ligne peuvent ne tenir à la disposition du public, pour préserver leur anonymat, que le nom, la dénomination ou la raison sociale et l'adresse de l'hébergeur sous réserve de lui avoir communiqué les éléments d'identification personnelle telles que prévues à l'Article 660.

Article 662 Espace de contributions personnelles

Lorsque l'infraction résulte du contenu d'un message adressé par un internaute à un service de communication au public en ligne et mis par ce service à la disposition du

public dans un espace de contributions personnelles identifié comme tel, le directeur ou le codirecteur de publication ne peut pas voir sa responsabilité pénale engagée comme auteur principal s'il est établi qu'il n'avait pas effectivement connaissance du message avant sa mise en ligne ou si, dès le moment où il en a eu connaissance, il a agi promptement pour retirer ce message.

Article 663 Sanctions des fournisseurs de contenu

Est puni d'une peine d'emprisonnement maximum d'un an et d'une amende maximum de 35.000.000 DJF le non-respect par les fournisseurs de contenu des obligations définies aux Articles Article 660 à Article 662.

Section 5 : Cybercafés

Article 664 Identification préalable des usagers de cybercafé

L'accès au service Internet à partir d'un cybercafé situé sur le territoire national est soumis à l'identification préalable des usagers.

Les exploitants de cybercafé sont tenus de procéder à cette identification.

Article 665 Accès restreint aux mineurs de moins de dix ans

Le mineur de moins de dix (10) ans ne peut accéder au cybercafé qu'accompagné d'un adulte.

L'accès à Internet dans un cybercafé pour un mineur de moins de dix-huit (18) ans est un accès limité, qui exclut les sites web à caractère pornographique, violent, raciste ou dégradant et de manière générale tous les sites web portant atteinte à la dignité humaine ou incitant à l'incivisme.

Chapitre 10 : Responsabilité pénale des personnes morales

Article 666 Responsabilité pénale de certaines personnes morales

Les personnes morales autres que la République de Djibouti, les collectivités publiques et les établissements publics sont pénalement responsables des infractions prévues par le Livre Sixième, commises pour leur compte par leurs organes ou représentants.

La responsabilité des personnes morales n'exclut pas celle des personnes physiques auteurs, instigateurs ou complices des mêmes faits.

Les peines encourues par les personnes morales sont :

1. L'amende dont le taux maximum est égal au quintuple de celui prévu pour les personnes physiques par la loi qui réprime l'infraction ;

2. La dissolution, lorsque la personne morale a été créée ;

3. L'interdiction à titre définitif ou pour une durée de cinq (5) ans au plus d'exercer directement ou indirectement une ou plusieurs activités professionnelles ou sociales ;

4. La fermeture définitive ou pour une durée de cinq (5) ans au plus d'un ou plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ;

5. L'exclusion des marchés publics à titre définitif ou pour une durée de cinq (5) ans au plus ;

6. L'interdiction à titre définitif ou pour une durée de cinq (5) ans au plus de faire appel public à l'épargne ;

7. L'interdiction pour une durée de cinq (5) ans au plus d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tire ou ceux qui sont certifies ou d'utiliser des cartes de paiement ;

8. La confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit ;

9. L'affichage de la décision prononcée ou la diffusion de celle-ci soit par la presse écrite soit par tout moyen de communication au public par voie électronique.

Article 667 Peines complémentaires

S'il y a condamnation pour une infraction commise par le biais d'un support de communication numérique, la juridiction peut prononcer à titre de peines complémentaires l'interdiction d'émettre des messages de communication numérique, l'interdiction à titre provisoire ou définitif de l'accès au site ayant servi à commettre l'infraction.

Le juge peut ordonner à toute personne responsable légalement du site ayant servi à commettre l'infraction, à toute personne qualifiée de mettre en œuvre les moyens techniques nécessaires en vue de garantir, l'interdiction d'accès, d'hébergement ou la coupure de l'accès au site incriminé.

La violation des interdictions prononcées par le juge sera punie d'une peine d'emprisonnement maximum de 3 ans et d'une amende maximum de 3.500.000 DJF.

Article 668 Diffusion aux frais du condamné de la décision de justice

En cas de condamnation à une infraction commise par le biais d'un support de communication numérique, le juge ordonne à titre complémentaire la diffusion aux frais du condamné, par extrait, de la décision sur ce même support.

La publication prévue à l'alinéa précédent doit être exécutée dans les quinze (15) jours suivant le jour où la condamnation est devenue définitive.

Le condamné qui ne fera pas diffuser ou qui ne diffusera pas l'extrait prévu à l'alinéa 1 sera puni des peines prévues par l'Article 667.

Titre 2 De la procédure en matière d'infractions commises au moyen des technologies de l'information et de la communication

Chapitre 1 : Des perquisitions

Article 669 Perquisition et accès à un système informatique contenant des données utiles à la manifestation de la vérité

Lorsque des données stockées dans un système informatique ou dans un support permettant de conserver des données informatisées sur le territoire djiboutien, sont utiles à la manifestation de la vérité, le juge d'instruction peut opérer une perquisition ou accéder à un système informatique ou à une partie de celui-ci ou dans un autre système informatique, des lors que ces données sont accessibles à partir du système initial ou disponible pour le système initial.

S'il est préalablement avéré que ces données, accessibles à partir du système initial ou disponible pour le système initial, sont stockées dans un autre système informatique situé en dehors du territoire national, elles sont recueillies par le juge d'instruction, par voie de commission rogatoire internationale.

Article 670 Accès aux données par les officiers de police judiciaire

Les officiers de police judiciaire peuvent, par tout moyen, requérir toute personne susceptible :

1. D'avoir connaissance des mesures appliquées pour protéger les données auxquelles il est permis d'accéder dans le cadre de la perquisition ;

2. De leur remettre les informations permettant d'accéder aux données mentionnées au 1).

Le fait de s'abstenir de répondre dans les meilleurs délais à cette réquisition est puni d'une amende de 200.000 DJF.

Article 671 Nécessité du consentement

Les perquisitions prévues à l'Article 670 ne peuvent avoir lieu qu'avec le consentement exprès de la personne chez qui l'opération a lieu.

Cependant, si l'enquête est relative à un crime, le juge d'instruction peut, sur autorisation écrite, décider que la perquisition et la saisie seront effectuées sans l'assentiment de la personne.

Article 672 Copie de données utiles à la manifestation de la vérité

Lorsque le juge d'instruction découvre dans un système informatique des données stockées qui sont utiles pour la manifestation de la vérité, mais que la saisie du support ne paraît pas souhaitable, ces données, de même que celles qui sont nécessaires pour les comprendre, sont copiées sur des supports de stockage informatique pouvant être saisis et placés sous scellés.

Chapitre 2 : De la conservation rapide des données

Article 673 Injonction de conserver et protéger l'intégrité de certaines données

Si les nécessités de l'information l'exigent, notamment lorsqu'il y a des raisons de penser que des données informatisées archivées dans un système informatique sont particulièrement susceptibles de perte ou de modification, le juge d'instruction peut faire injonction à toute personne de conserver et de protéger l'intégrité des données en sa possession ou sous son contrôle, pendant une durée de deux (2) ans maximum, pour la bonne marche des investigations judiciaires.

Le gardien des données ou toute autre personne chargée de conserver celles-ci est tenu d'en garder le secret.

Toute violation du secret est punie des peines applicables au délit de violation du secret de l'instruction.

Chapitre 3 : De l'interception des données informatisées

Article 674 Collecte et enregistrement en temps réel de données

Si les nécessités de l'information l'exigent, le juge d'instruction peut ordonner d'office après avis du procureur de la République de Djibouti ou sur réquisition du procureur de la République de Djibouti, à toute autorité compétente de collecter ou enregistrer en temps réel, les données relatives au contenu de communications spécifiques, transmises

au moyen d'un système informatique ou obliger un fournisseur de services, dans le cadre de ses capacités techniques à collecter ou à enregistrer, ou à prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer lesdites données informatisées. Le fournisseur d'accès est tenu de garder le secret. Toute violation du secret est punie des peines applicables au délit de violation du secret professionnel.

Article 675 Pouvoirs de l'officier de police judiciaire

L'officier de police judiciaire peut, pour les nécessités de l'enquête ou de l'exécution d'une délégation judiciaire, procéder aux opérations prévues par les Article 669 à Article 674.

Chapitre 4 : Compétences des juridictions djiboutiennes en matière de cybercriminalité

Article 676 Compétences des juridictions djiboutiennes

Sans préjudice des Articles 9 à 19 du Code pénal, les juridictions djiboutiennes sont compétentes lorsque :

1. l'infraction a été commise sur Internet sur le territoire de la République de Djibouti dès lors que le contenu illicite est accessible depuis la République de Djibouti ;

2. l'infraction a été commise sur le territoire de la République de Djibouti, y compris les espaces maritimes et aériens ;

3. une personne physique ou morale s'est rendue coupable sur le territoire de la République de Djibouti, comme instigateur ou complice, d'un crime ou d'un délit commis à l'étranger si le crime ou le délit est puni à la fois par la loi djiboutienne et par la loi étrangère et s'il a été constaté par une décision définitive de la juridiction étrangère ;

4. le crime a été commis par des personnes de nationalité djiboutienne hors du territoire de la République de Djibouti ;

5. le délit a été commis par des personnes de nationalité djiboutienne hors du territoire de la République de Djibouti , si les faits sont punis par la législation du pays où ils ont été commis ;

6. tout crime ou délit puni d'emprisonnement, a été commis par une personne de nationalité djiboutienne ou par un étranger hors du territoire de la République de

Djibouti lorsque la victime est de nationalité djiboutienne au moment de l'infraction.

Chapitre 5 : De la prescription des infractions commises sur internet

Article 677 Application des prescriptions du Code pénal

Les dispositions de la Section I du Chapitre III du Livre III du Code pénal relatif à la prescription seront applicables aux infractions commises au moyen d'un ou sur un réseau de communications électroniques ou un système informatique.

Chapitre 6 : Du droit de réponse sur internet

Article 678 Droit de réponse

Toute personne nommée ou désignée au moyen d'un ou sur un réseau de communication électronique ou un système informatique, dispose d'un droit de réponse, sans préjudice des demandes de correction ou de suppression du message qu'elle peut adresser au service.

Elle est présentée au plus tard dans un délai de trois (3) mois à compter de la mise à disposition du public du message justifiant cette demande.

Le directeur de la publication est tenu d'insérer dans les trois (3) jours de leur réception les réponses de toute personne nommée ou désignée dans le service de communication au public en ligne sous peine d'une amende de 300.000 DJF.

Titre 3 De la mise en œuvre de la défense non militaire et non économique

Chapitre 1 : Protection des installations

Article 679 Systèmes qualifiés de détection des évènements susceptibles d'affecter la sécurité des systèmes d'information

Les opérateurs sont tenus de mettre en œuvre des systèmes qualifiés de détection des événements susceptibles d'affecter la sécurité de leurs systèmes d'information.

Les qualifications des systèmes de détection et des prestataires de service exploitant ces systèmes sont délivrés par l'Autorité nationale en charge de la cybersécurité selon les modalités prévues à l'Article 390.

Article 680 Contrôles de vérification du niveau de sécurité

Les opérateurs doivent soumettre leurs systèmes d'information à des contrôles destinés à vérifier le niveau de sécurité et le respect des règles de sécurité. Les contrôles sont effectués par l'Autorité nationale en chargede la cybersécurité. Le coût des contrôles est à la charge de l'opérateur.

Article 681 Sanctions

Est puni d'une amende de 10.000.000 DJF le fait, pour les mêmes personnes, d'omettre d'entretenir et de maintenir en bon état les dispositifs de protection antérieurement établis.

Chapitre 2 : Sécurité des systèmes informatiques

Article 682 Détention de matériels et données permettant de répondre aux attaques informatiques

Pour être en mesure de répondre à une attaque informatique, les services de la République du Djibouti désignés par décret pris en Conseil des ministres peuvent détenir des équipements, des instruments, des programmes informatiques et toutes données susceptibles de permettre la réalisation d'une ou plusieurs des infractions en vue d'analyser leur conception et d'observer leur fonctionnement.

Article 683 Obtention de données sur certains utilisateurs

Pour les besoins de la sécurité des systèmes d'information et des opérateurs, l'autorité compétente désignée par décret pris en Conseil des ministres peut obtenir des opérateurs de communications électroniques l'identité, l'adresse postale et l'adresse électronique d'utilisateurs ou de détenteurs de systèmes d'information vulnérables, menacés ou attaqués, afin de les alerter sur la vulnérabilité ou la compromission de leur système.

Article 684 Sanctions

Le fait de faire obstacle à l'accomplissement des missions prévues auxArticle 682 etArticle 683 est puni d'une amende de 25.000.000 DJF.

Livre Septième : Services numériques innovants

Titre 1 Echanges avec l'administration par voie électronique

Chapitre 1 : Dispositions générales

Article 685 Champ d'application

Le présent Titre a pour objet de définir le cadre de création et de mise en œuvre, par l'administration, des téléservices permettant aux usagers d'accomplir certaines formalités administratives et de bénéficier de services délivrés par voie électronique.

Le présent Titre a également pour objet de simplifier les formalités auxquelles les usagers sont assujettis et de définir les référentiels d'interopérabilité des systèmes d'information utilisés pour les téléservices.

Les systèmes d'information relevant du secret de la défense nationale sont exclus du champ d'application du présent Titre.

Article 686 Identification de l'interlocuteur

Toute personne a le droit de connaître le prénom, le nom, la qualité et l'adresse administrative de l'agent chargé d'instruire sa demande ou de traiter l'affaire qui la concerne. Ces éléments figurent sur les correspondances qui lui sont adressées.

Par exception, et pour des motifs relevant de la sécurité publique ou la sécurité des personnes, l'anonymat de l'agent est respecté.

Article 687 Réponse de l'administration par voie électronique

L'administration peut répondre par voie électronique à toute demande et à tout envoi d'information ou de document fait par une personne ou par une autre administration, sauf refus exprès de l'intéressé.

Chapitre 2 : Modalités de saisine de l'administration par voie électronique et mise en place de téléservices

Section 1 : Saisine par voie électronique et téléservices

Article 688 Droit de saisir ou de répondre à l'administration par voie électronique

Toute personne, dès lors qu'elle s'est identifiée préalablement auprès d'une administration, peut adresser à celle-ci par voie électronique, une demande, une déclaration, un document ou une information, ou lui répondre par voie électronique.

L'administration est alors régulièrement saisie et traite la demande, la déclaration, le document ou l'information sans demander la confirmation ou la répétition de l'envoi sous une autre forme.

Article 689 Mise en place de téléservices par l'administration

L'administration met en place un ou plusieurs téléservices, dans le respect des dispositions du Livre Premier.

Lorsqu'elle met en place un ou plusieurs téléservices, l'administration rend accessibles leurs modalités d'utilisation, notamment les modes de communication possibles. Ces modalités s'imposent au public.

Lorsqu'elle a mis en place un téléservice réservé à l'accomplissement de certaines démarches administratives, une administration n'est régulièrement saisie par voie électronique que par l'usage de ce téléservice.

Lorsqu'une formalité est exigée par la législation ou la réglementation en vigueur, l'administration concernée met en œuvre les moyens techniques sécurisés permettant aux personnes d'accomplir lesdites formalités par voie électronique.

Article 690 Adaptation des téléservices aux personnes ayant des besoins spécifiques

Les dispositions du présent article s'appliquent vis-à-vis des personnes présentant un handicap entraînant des besoins spécifiques en matière de communications électroniques, en particulier les personnes sourdes, malentendantes, aveugles ou aphasiques.

L'administration prend les mesures nécessaires pour rendre accessible ses téléservices aux personnes handicapées, par tout moyen adapté à leur handicap.

La mise en œuvre de cette obligation peut s'appuyer sur des applications de communications électroniques permettant la vocalisation du texte, la transcription de la

voix en texte, la traduction en et depuis la langue des signes française ou la transcription en et depuis le langage parlé et complété.

Article 691 Mise en place de points d'accès aux téléservices

L'ensemble des téléservices est accessible à partir d'un portail électronique mis en place par l'Etat, dont les modalités de mise en œuvre sont fixées par décret pris en Conseil des ministres.

Article 692 Recueil des téléservices

L'administration informe le public par tout moyen des téléservices qu'elle met en place.

A défaut d'information sur le ou les téléservices mis en place, le public peut saisir l'administration par tout type d'envoi électronique.

Article 693 Exception à l'utilisation des téléservices

L'utilisation des téléservices pour certaines démarches administratives peut être écartée par décret pris en Conseil des ministres, pour des motifs d'ordre public, de défense et de sécurité nationale, de bonne administration, ou lorsque la présence personnelle de la personne présentant une demande ou effectuant une déclaration apparaît nécessaire.

Section 2 : Accusé de réception des demandes formées par voie électronique

Article 694 Principe général

Tout envoi à une administration par voie électronique ainsi que tout paiement opéré dans le cadre d'un téléservice fait l'objet d'un accusé de réception électronique ou d'un accusé d'enregistrement électronique.

Article 695 Exceptions

L'administration n'est pas tenue de respecter l'obligation prévue à l'Article 694 pour les envois abusifs, notamment par leur nombre ou leur caractère répétitif ou systématique, ou pour les envois susceptibles de porter atteinte à la sécurité de son système d'information.

Après en avoir, si possible, informé la source des envois en cause, un système d'information peut être configuré pour bloquer la réception des envois provenant de sources identifiées comme ayant émis un nombre significatif d'envois abusifs ou susceptibles de porter atteinte à la sécurité du système d'information.

Article 696 Caractéristiques de l'accusé de réception ou d'enregistrement électronique

L'accusé de réception ou d'enregistrement électronique prévu à l'Article 694 comporte les mentions suivantes, pouvant être complétées par décret pris en Conseil des ministres

1. La date de réception de l'envoi électronique effectué par la personne ;

2. La désignation du service chargé du dossier, ainsi que son adresse électronique ou postale et son numéro de téléphone.

S'il s'agit d'une demande, l'accusé de réception ou d'enregistrement indique en outre si la demande est susceptible de donner lieu à une décision implicite d'acceptation ou à une décision implicite de rejet ainsi que la date à laquelle, à défaut d'une décision expresse, et sous réserve que la demande soit complète, celle-ci sera réputée acceptée ou rejetée. Il mentionne également les délais et les voies de recours à l'encontre de la décision.

Article 697 Modalités d'envoi de l'accusé de réception

Tout envoi à l'administration par voie électronique et tout paiement dans le cadre d'un téléservice, fait l'objet d'un accusé de réception ou d'enregistrement électronique de façon instantanée, ou au plus tard dans un délai d'un (1) jour ouvré.

L'accusé de réception électronique et l'accusé d'enregistrement électronique sont adressés à l'intéressé à l'adresse électronique qu'il a utilisée pour effectuer son envoi, sauf mention d'une autre adresse donnée à cette fin.

Article 698 Certification de la date d'envoi

Toute personne tenue de respecter une date limite ou un délai pour présenter une demande, déposer une déclaration, effectuer un paiement ou produire un document auprès d'une administration peut satisfaire à cette obligation au moyen d'un envoi par voie électronique, et au plus tard à la date prescrite. Dans ce cas, la date figurant sur l'accusé de réception ou sur l'accusé d'enregistrement adressé à l'usager fait foi.

Ces dispositions ne sont pas applicables :

1. Aux procédures d'attribution des contrats administratifs ayant pour objet l'exécution de travaux, la livraison de fournitures ou la prestation de services, avec une contrepartie économique constituée par un prix ou un droit d'exploitation ;

2. Aux procédures pour lesquelles la présence personnelle du demandeur est exigée en application d'une disposition particulière.

Article 699 Saisine d'une administration compétente

Lorsqu'une demande est adressée à une administration incompétente, cette dernière la transmet à l'administration compétente et en avise l'intéressé.

Le délai au terme duquel est susceptible d'intervenir une décision implicite de rejet ou d'acceptation ne court qu'à compter de la date de réception de la demande par l'administration compétente. Si cette administration informe l'auteur de la demande qu'il n'a pas fourni l'ensemble des informations ou pièces exigées, le délai ne court qu'à compter de la réception de ces informations ou pièces.

L'accusé de réception ou d'enregistrement électronique est délivré par l'administration compétente.

Chapitre 3 : Soumission ou notification de documents par voie électronique

Article 700 Règles générales

Lorsqu'une personne doit adresser un document à l'administration par lettre recommandée, cette formalité peut être accomplie par l'utilisation d'un téléservice, d'un envoi recommandé électronique tel que défini au Livre Préliminaire du présent Code ou d'un procédé électronique accepté par cette administration, permettant de désigner l'expéditeur et d'établir si le document lui a été remis.

Lorsque l'administration doit notifier un document à une personne par lettre recommandée, cette formalité peut être accomplie par l'utilisation d'un envoi recommandé électronique tel que défini au Livre Préliminaire du présent Code ou d'un procédé électronique permettant de désigner l'expéditeur, de garantir l'identité du destinataire et d'établir si le document a été remis. L'accord exprès de l'intéressé doit être préalablement recueilli.

Article 701 Information par l'administration sur les modalités d'échange de document par voie électronique

L'administration informe le public du ou des procédés électroniques qu'elle accepte, équivalents à la lettre recommandée et conformes aux règles fixées par le référentiel général d'interopérabilité et de sécurité prévu à l'Article 709 .

Article 702 Consentement à la notification de documents par voie électronique

Après accord exprès de la personne recueilli par voie électronique, celle-ci choisit, le cas échéant, parmi les moyens que lui propose l'administration, celui par lequel elle désire recevoir les avis de dépôt de documents électroniques qui lui sont adressés. Elle maintient à jour ses coordonnées par la même voie, afin que les avis de dépôt de documents électroniques puissent lui parvenir.

Si elle ne souhaite plus bénéficier du procédé électronique, elle en informe l'administration par voie électronique. Sa requête doit être prise en compte par l'administration dans un délai qui ne peut excéder trois (3) mois.

Article 703 Notification de documents consultables électroniquement

L'administration adresse à la personne un avis l'informant qu'un document est mis à sa disposition, et qu'elle peut en prendre connaissance par le procédé prévu à l'Article 701 . Cet avis mentionne la date de mise à disposition du document, les coordonnées du service expéditeur et le délai prévu à l'Article 704.

Article 704 Date de consultation de documents conservés électroniquement

Le document notifié est réputé avoir été reçu par son destinataire à la date de sa première consultation. Cette date peut être consignée dans un accusé de réception adressé à l'administration par le procédé prévu à l'Article 701.

A défaut de consultation du document par son destinataire dans un délai de quinze (15) jours, le document est réputé lui avoir été notifié à la date de mise à disposition.

Chapitre 4 : Informations fournies à l'administration

Article 705 Mise à disposition de formulaires électroniques

Les formulaires dont l'usage est nécessaire pour accomplir une démarche auprès d'une administration sont tenus gratuitement à la disposition du public, sous forme numérique.

L'administration ne peut refuser d'examiner une demande présentée au moyen d'un formulaire disponible sous forme électronique dès lors que ce formulaire, dûment rempli, n'a fait l'objet d'aucune altération par rapport aux données figurant sur le site sur lequel il est mis à disposition du public.

Article 706 Exception à l'exigence de certification conforme

L'administration ne peut exiger la certification conforme à l'original des photocopies de documents délivrés par une administration et pour lesquelles une simple photocopie n'est pas déjà admise par un texte législatif ou réglementaire.

Toutefois l'administration peut, sur demande, procéder à la certification de photocopies de documents demandées par des autorités étrangères.

Article 707 Recours à l'envoi de documents sur support papier

En cas de doute sur la validité de la pièce justificative envoyée par voie électronique par toute personne présentant une demande ou effectuant une déclaration, l'administration

peut adresser à la personne concernée une demande motivée de présentation de la pièce originale.

La procédure en cours est suspendue jusqu'à la production des pièces originales demandées.

Chapitre 5 : Echange de données entre administrations

Article 708 Principe général

Les administrations échangent entre elles toutes les informations ou données strictement nécessaires pour traiter une demande ou une déclaration transmise en application d'un texte législatif ou réglementaire.

Les administrations destinataires de ces informations ou données ne peuvent se voir opposer le secret professionnel dès lors qu'elles sont, dans le cadre de leurs missions légales, habilitées à connaître des informations ou des données ainsi échangées.

Une administration chargée de traiter une demande ou une déclaration fait connaître à la personne concernée les informations ou données nécessaires à cette fin. L'administration informe également la personne concernée des informations ou données qu'elle se procure directement auprès d'autres administrations de l'Etat, qui en sont à l'origine ou qui les détiennent en vertu de leur mission.

Toute personne est informée du droit d'accès et de rectification dont elle dispose sur les informations et données mentionnées au présent article.

Article 709 Référentiel général d'interopérabilité et de sécurité des téléservices

Un référentiel général d'interopérabilité et de sécurité fixe les règles techniques permettant d'assurer l'interopérabilité des systèmes d'information utilisés pour les téléservices. Il détermine notamment les répertoires de données, les normes et les standards applicables.

Les dispositions de mise en œuvre du référentiel général d'interopérabilité et de sécurité des téléservices font l'objet d'un décret pris en Conseil des ministres.

Article 710 Conformité avec le référentiel général d'interopérabilité et de sécurité des téléservices

L'administration s'assure et atteste formellement que le système d'information utilisé pour la mise en œuvre des téléservices est protégé conformément au référentiel général de sécurité et d'interopérabilité prévu par l'Article 709.

Cette information est rendue accessible sur la page d'accueil du téléservice concerné.

Article 711 Sécurité et traçabilité des échanges

Les informations relevant du présent Titre sont mises à disposition par l'administration sous forme électronique par le biais de traitements automatisés assurant la traçabilité et la sécurité des échanges.

Titre 2 Accès aux documents administratifs et réutilisation des données publiques

Chapitre 1 : Droit d'accès aux documents administratifs

Section 1 : Dispositions générales

Article 712 Définition

Sont considérés comme documents administratifs au sens du présent Titre, quels que soient leur date, leur lieu de conservation, leur forme et leur support, les documents produits ou reçus dans le cadre de leur mission de service public par l'Etat, les collectivités territoriales, par les autres personnes de droit public, ou par les personnes de droit privé chargées d'une mission de service public. Constituent notamment de tels documents les dossiers, rapports, études, comptes rendus, procès-verbaux, statistiques, instructions, circulaires, notes et réponses ministérielles, correspondances, avis, prévisions, codes sources et décisions.

Article 713 Désignation d'une personne responsable de l'accès aux documents administratifs et à la réutilisation de données publiques

Les administrations mentionnées à l'Article 712 sont tenues de désigner une personne responsable de l'accès aux documents administratifs sous forme électronique et des questions relatives à la réutilisation des informations publiques. Un décret pris en Conseil des ministres détermine les conditions de désignation et d'exercice du responsable.

Section 2 : Communication des documents administratifs

Article 714 Obligation de communication

Les administrations peuvent communiquer par voie électronique les documents administratifs qu'elles détiennent aux personnes qui en font la demande, dans les conditions prévues par le présent Titre.

Article 715 Exclusions

Le droit à communication par voie électronique ne concerne pas les documents préparatoires à une décision administrative tant qu'elle est en cours d'élaboration.

Le droit à communication par voie électronique ne s'exerce plus lorsque les documents font l'objet d'une diffusion publique.

L'administration n'est pas tenue de donner suite aux demandes abusives, en particulier par leur nombre ou leur caractère répétitif ou systématique.

Article 716 Restrictions au droit d'accès aux documents administratifs pour des raisons d'intérêt public

Ne sont pas communicables par voie électronique les documents administratifs dont la consultation ou la communication porterait atteinte :

1. Au secret des délibérations du Gouvernement et des autorités responsables relevant du pouvoir exécutif ;
2. Au secret de la défense nationale ;
3. A la conduite de la politique extérieure de la République de Djibouti ;
4. A la sûreté de l'Etat, à la sécurité publique, à la sécurité des personnes ou à la sécurité des systèmes d'information des administrations ;
5. A la monnaie et au crédit public ;
6. Au déroulement des procédures engagées devant les juridictions ou d'opérations préliminaires à de telles procédures, sauf autorisation donnée par l'autorité compétente ;
7. A la recherche et à la prévention, par les services compétents, d'infractions de toute nature;
8. Aux autres secrets protégés par la loi.

Nonobstant l'alinéa précédent, ces documents administratifs peuvent être communiqués par voie électronique aux conditions et au terme d'un délai fixé par un décret pris en Conseil des ministres sur proposition du ministère en charge de l'économie numérique.

Article 717 Restrictions au droit d'accès aux documents administratifs pour des raisons d'intérêt privé

Ne sont communicables par voie électronique qu'à l'intéressé les documents administratifs :

1. Dont la communication porterait atteinte à la protection de la vie privée, au secret médical ou au secret des affaires, lequel comprend le secret des procédés, des informations économiques et financières et des stratégies commerciales ou industrielles et est apprécié en tenant compte, le cas échéant, du fait que la

mission de service public de l'administration mentionnée à l'Article 712 est soumise à la concurrence ;

2. Portant une appréciation ou un jugement de valeur sur une personne physique, nommément désignée ou facilement identifiable ;

3. Faisant apparaître le comportement d'une personne, dès lors que la divulgation de ce comportement pourrait lui porter préjudice.

Les informations à caractère médical sont communiquées directement à l'intéressé, ou selon son choix, par l'intermédiaire d'un médecin qu'il désigne à cet effet.

Article 718 Occultation des mentions non communicables

Lorsque la demande de communication porte sur un document comportant des mentions qui ne sont pas communicables en application des Article 716 et Article 717 mais qu'il est possible d'occulter ou de retirer, le document est communiqué par voie électronique au demandeur après occultation ou retrait de ces mentions.

Article 719 Préservation des droits de propriété intellectuelle

Les documents administratifs sont communiqués par voie électronique ou publiés électroniquement sous réserve des droits de propriété littéraire et artistique applicables.

Article 720 Modalités d'exercice du droit d'accès

L'accès aux documents administratifs peut s'exercer, au choix du demandeur et dans la limite des possibilités techniques de l'administration :

1. Par la délivrance d'une copie sur un support identique à celui utilisé par l'administration ou compatible avec celui-ci, sous réserve que la reproduction ne nuise pas à la conservation du document. La reproduction est faite aux frais du demandeur, sans que ces frais puissent excéder le coût de cette reproduction, et dans des conditions prévues par décret pris en Conseil des ministres ;

2. Par courrier électronique et sans frais lorsque le document est disponible sous forme électronique ;

3. Par publication des informations en ligne, à moins que les documents ne soient communicables qu'à l'intéressé en application de l'Article 717.

Article 721 Transmission sur support électronique

Lorsqu'un document est détenu par l'une des administrations mentionnées à l'Article 712 sur un support électronique et que le demandeur souhaite en obtenir copie sur un support identique ou compatible avec celui utilisé par cette administration, celle-ci

indique au demandeur les caractéristiques techniques de ce support. Elle lui indique également si le document peut être transmis par voie électronique.

Article 722 Refus de communication

Toute décision de refus d'accès aux documents administratifs par voie électronique est notifiée au demandeur.

Section 3 : Diffusion des documents administratifs

Article 723 Droit de rendre public certains documents administratifs

Les administrations mentionnées à l'Article 712 peuvent rendre publique les documents administratifs qu'elles produisent ou reçoivent.

Article 724 Obligation de publication en ligne

Sous réserve des Article 716 et Article 717 et lorsque ces documents sont disponibles sous forme électronique, les administrations mentionnées à l'Article 717 publient en ligne les documents administratifs suivants :

1. Les documents qu'elles communiquent en application des procédures prévues au présent Titre, ainsi que leurs versions mises à jour ;

2. Les bases de données, mises à jour de façon régulière, qu'elles produisent ou qu'elles reçoivent et qui ne font pas l'objet d'une diffusion publique par ailleurs ;

3. Les données, mises à jour de façon régulière, dont la publication présente un intérêt économique, social, sanitaire ou environnemental.

Article 725 Occultation des mentions non communicables

Sauf dispositions législatives ou réglementaires contraires, lorsque les documents et données mentionnés aux Article 723 et Article 724 comportent des mentions entrant dans le champ d'application des Article 716 et Article 717, ils ne peuvent être rendus publics en ligne qu'après avoir fait l'objet d'un traitement permettant d'occulter ces mentions.

Sauf dispositions législatives ou réglementaires contraires ou si les personnes intéressées ont donné leur accord, lorsque les documents et les données mentionnés aux Article 723 et Article 724 comportent des données à caractère personnel, ils ne peuvent être rendus publics qu'après avoir fait l'objet d'un traitement permettant de rendre impossible l'identification de ces personnes. Une liste des catégories de documents pouvant être rendus publics sans avoir fait l'objet du traitement susmentionné est fixée par décret pris en Conseil des ministres sur proposition du ministère en charge de l'économie

numérique, après avis de la Commission Nationale de Protection des Données à Caractère Personnel.

Article 726 Exception à l'obligation de rendre impossible l'identification de personnes identifiables

Les documents et informations mentionnés aux Article 723 et Article 724 et qui sont communicables ou accessibles à toute personne, sous réserve des Article 716 et Article 717 et d'autres dispositions législatives ou réglementaires en vigueur, peuvent être rendus publics en ligne sans avoir fait l'objet du traitement prévu au deuxième alinéa de l'Article 718, lorsqu'ils relèvent de l'une des catégories suivantes :

1. Les documents nécessaires à l'information du public relatifs aux conditions d'organisation de l'administration, notamment les organigrammes, les annuaires des administrations et la liste des personnes inscrites à un tableau d'avancement ou sur une liste d'aptitude pour l'accès à un échelon, un grade ou un corps ou cadre d'emplois de la fonction publique ;

2. Les documents nécessaires à l'information du public relatifs aux conditions d'organisation de la vie économique, associative et culturelle, notamment le Registre national de l'économie sociale et solidaire ;

3. Les documents nécessaires à l'information du public relatifs aux conditions d'organisation et d'exercice des professions réglementées et des activités professionnelles soumises à la règlementation, notamment celles relatives à l'exercice des professions de notaire, avocat, huissier de justice et architecte ;

4. Les documents nécessaires à l'information du public relatifs à l'enseignement et la recherche, notamment les résultats obtenus par les candidats aux examens et concours administratifs, ou conduisant à la délivrance de diplômes nationaux ;

5. Les documents nécessaires à l'information du public relatifs aux conditions d'organisation et d'exercice des activités sportives ;

6. Les documents nécessaires à l'information du public relatifs aux conditions d'organisation et d'exercice de la vie politique ;

7. Les documents nécessaires à l'information du public relatifs aux conditions d'organisation et d'exercice des activités touristiques ;

8. Les documents nécessaires à l'information du public relatifs aux activités soumises à des formalités prévues par des dispositions législatives ou réglementaires, notamment en matière d'urbanisme, d'occupation du domaine public et de protection des données à caractère personnel ;

9. Les documents administratifs conservés par les services publics d'archives et les autres organismes chargés d'une mission de service public d'archivage, selon des conditions fixées par décret pris en Conseil des ministres.

Chapitre 2 : Réutilisation des données publiques

Article 727 Droit de propriété intellectuelle des administrations

Sous réserve de droits de propriété intellectuelle détenus par des tiers, les droits des administrations mentionnées à l'Article 712 ne peuvent faire obstacle à la réutilisation du contenu des bases de données que ces administrations peuvent être amenées à publier.

Le premier alinéa du présent article n'est pas applicable aux bases de données produites ou reçues par les administrations mentionnées à l'Article 712 dans l'exercice d'une mission de service public à caractère industriel ou commercial soumise à la concurrence.

Article 728 Conditions générales de réutilisation des données publiques

Sauf accord de l'administration, la réutilisation des informations publiques en ligne est soumise à la condition que ces dernières ne soient pas altérées, que leur sens ne soit pas dénaturé et que leurs sources et la date de leur dernière mise à jour soient mentionnées.

Article 729 Recueil des données publiques ouvertes à la réutilisation

Les administrations qui produisent ou détiennent des informations publiques en ligne tiennent à la disposition des usagers un recueil des principaux documents dans lesquels ces informations figurent. Elles publient chaque année une version mise à jour de ce recueil.

Article 730 Sanctions

Toute personne réutilisant des informations publiques en violation des prescriptions du présent Chapitre est passible d'une amende dont le montant est fixé par décret pris en Conseil des ministres.

Lorsque des informations publiques en ligne ont été réutilisées à des fins commerciales en méconnaissance des dispositions du présent Chapitre, le montant de l'amende est proportionné à la gravité du manquement commis et aux avantages tirés de ce manquement.

Titre 3 Organisation de la mise à disposition des données de santé

Chapitre 1 : Principes généraux

Article 731 Utilisation obligatoire du numéro d'identification national comme identifiant national de santé

Le numéro d'inscription au registre national d'identification des personnes physiques est utilisé comme identifiant national de santé des personnes pour leur prise en charge à des fins sanitaires et médico-sociales.

L'identification des personnes par leur numéro d'identification nationale et l'utilisation de ce numéro comme identifiant de santé est obligatoire.

Article 732 Objets de l'utilisation de l'identifiant national de santé

L'identifiant national de santé est utilisé pour référencer les données de santé et les données administratives de toute personne bénéficiant ou appelée à bénéficier d'un acte diagnostique, thérapeutique, de prévention, de soulagement de la douleur, de compensation d'un handicap, de prévention de la perte d'autonomie, ou d'interventions nécessaires à la coordination de plusieurs de ces actes.

Article 733 Conditions d'utilisation de l'identifiant de santé

L'utilisation de l'identifiant national de santé afin de référencer les données de santé ne peut être réalisée que par des professionnels, établissements, services ou organismes de santé, de soins ou du secteur médico-social, et intervenant dans la prise en charge sanitaire ou médico-sociale de la personne concernée.

Article 734 Traitement des données de santé aux fins de recherche, étude ou évaluation

Les données de santé ayant pour finalité la recherche ou les études dans le domaine de la santé ainsi que l'évaluation ou l'analyse des pratiques ou des activités de soin ou de prévention, peuvent faire l'objet de traitements automatisés de données dans les conditions édictées à l'Article 80 du présent Code.

Ces traitements ne peuvent avoir ni pour objet ni pour effet de porter atteinte à la vie privée des personnes concernées, ni de permettre leur identification directe ou indirecte.

Article 735 Droit d'accès aux données de santé

Conformément à l'Article 34 du présent Code, la personne concernée par les données de santé conservées et mentionnées à l'Article 738peut y avoir accès directement ou par l'intermédiaire d'un médecin de son choix. En cas de décès de la personne concernée,

ses ayants-droits peuvent exercer ce droit d'accès aux données par l'intermédiaire d'un médecin qu'ils désignent.

Article 736 Interdiction de cession de données de santé identifiantes

Tout acte de cession à titre onéreux de données de santé permettant d'identifier directement ou indirectement la personne concernée est interdit, y compris avec l'accord de la personne concernée sous peine de cinq (5) ans d'emprisonnement et d'une amende de 4.500.000 DJF, ou de l'une de ces peines seulement.

Chapitre 2 : Système national des données de santé

Article 737 Création et contenu du système national de données de santé

Le système national des données de santé est mis en œuvre dans le cadre d'orientations générales définies par décret pris en Conseil des ministres, après avis de la Commission Nationale de Protection des Données à Caractère Personnel du Ministère de la santé et du ministère en charge de l'économie numérique, en concertation avec l'Autorité de la cybersécurité.

Article 738 Catégories de données réunies dans le système national de données de santé

Le système national des données de santé réunit :

1. Les données issues des systèmes d'information des établissements de santé publics ou privés dans le cadre de l'analyse de leur activité ;

2. Les données du système national d'information de l'assurance maladie ;

3. Les données sur les causes de décès établies sur les certificats transmis à l'administration ;

4. Les données relatives aux personnes atteintes d'un handicap ;

5. Un échantillon représentatif des données de remboursement par bénéficiaire transmises par des organismes soumis au régime d'assurance maladie complémentaire ;

6. Les données destinées aux professionnels et organismes de santé recueillies à l'occasion d'activités de prévention, de diagnostic, thérapeutiques, de soins ou de suivi social et médico-social, pour le compte de personnes physiques ou morales à l'origine de la production ou du recueil de ces données ou pour le compte du patient lui-même, donnant lieu à la prise en charge des frais de santé en matière de maladie, de maternité, d'accidents du travail ou de maladies professionnelles ;

7. Les données relatives à la perte d'autonomie lorsqu'elles viennent en complément des données mentionnées aux 1° à 6° du présent article ;

8. Les données à caractère personnel des enquêtes dans le domaine de la santé lorsqu'elles viennent en complément des données mentionnées aux 1° à 6° du présent article ;

9. Les données recueillies par les services de protection maternelle et infantile dans le cadre de leurs missions

10. Les données de santé recueillies lors des visites d'information et de prévention auprès des travailleurs

Article 739 Finalités du système national de données de santé

Le système national des données de santé a pour finalité la mise à disposition des données pour contribuer :

1. A l'information sur la santé ainsi que sur l'offre de soins, la prise en charge médico-sociale et leur qualité ;

2. A la définition, à la mise en œuvre et à l'évaluation des politiques de santé et de protection sociale ;

3. A la connaissance des dépenses de santé, des dépenses d'assurance maladie et des dépenses médico-sociales ;

4. A l'information des professionnels, des structures et des établissements de santé ou médico-sociaux sur leur activité ;

5. A la surveillance, à la veille et à la sécurité sanitaire ;

6. A la recherche, aux études, à l'évaluation et à l'innovation dans les domaines de la santé et de la prise en charge médico-sociale.

Article 740 Gestion du système national de données de santé

Le gestionnaire du système national de données de santé est défini par décret pris en Conseil des ministres. Pour le système national des données de santé et pour les traitements utilisant des données à caractère personnel issues de ce système :

1. Aucune décision ne peut être prise à l'encontre d'une personne physique identifiée sur le fondement des données la concernant et figurant dans l'un de ces traitements ;

2. Les personnes responsables du système national des données de santé, du traitement de ces données ainsi que celles mettant en œuvre ce traitement ou celles autorisées à accéder aux données, sont soumises au secret professionnel ;

3. L'accès aux données s'effectue dans des conditions assurant la confidentialité et l'intégrité des données ainsi que la traçabilité des accès et des traitements, conformément au référentiel mentionné à l'Article 745;

4. Les données individuelles du système national des données de santé sont conservées pour une durée maximale de vingt (20) ans, sans préjudice des dispositions édictées au Livre Premier du présent Code;

5. Le gestionnaire du système national de données de santé doit se conformer aux règles du référentiel établi selon l'Article 745 ainsi qu'aux dispositions édictées par le Livre Premier du présent Code. Il doit également réaliser, de manière périodique, un contrôle technique et fonctionnel du système national de données de santé et des systèmes d'informations permettant sa mise en œuvre.

6. Tout projet ayant un impact sur la sécurité du système national de données de santé, notamment une modification de l'architecture, l'inclusion de nouveaux types de données, ou d'un nouveau logiciel, ou une modification des conditions d'accès, doit donner lieu à une revue de l'analyse de risques du système. Si l'analyse met à jour l'apparition de nouveaux risques majeurs, une revue du système doit être réalisée.

Article 741 Traçabilité des données de santé et des opérations effectuées

Toutes les actions réalisées sur les données contenues dans le système national des données de santé, quel qu'en soit l'auteur, sont tracées et conservées dans le système, notamment la date, l'heure, et l'identité de la personne qui a créé ou modifié les données ou informations contenues dans le système. Ces traces sont accessibles à la personne concernée par les données recueillies et aux personnes mentionnées à l'Article 735.

Article 742 Exclusion des données identifiantes du système national de données de santé

Le système national des données de santé ne contient ni les noms et prénoms des personnes, ni leur numéro d'inscription au registre national d'identification des personnes physiques, ni leur adresse.

Les numéros d'identification des professionnels de santé sont conservés et gérés séparément des données de santé concernant les patients.

Article 743 Pseudonymisation des données de santé

Un procédé sécurisé doit être utilisé pour pseudonymiser les données de santé. Ce procédé doit être basé sur des fonctions cryptographiques répondant aux critères établis par décret pris en Conseil des ministres sur proposition du ministre en charge de l'économie numérique.

Chapitre 3 : Optimisation et sécurisation des données de santé

Article 744 Standardisation des données de santé

Les données de santé qui font l'objet d'une mise à la disposition du public sont traitées pour prendre la forme de statistiques agrégées ou de données individuelles constituées de telle sorte que l'identification, directe ou indirecte, des personnes concernées, est impossible.

Article 745 Référentiel général d'interopérabilité et sécurité du système national de données de santé

Un référentiel général d'interopérabilité et de sécurité fixe les règles techniques permettant d'assurer l'interopérabilité des systèmes d'information utilisés pour le système national de données de santé et pour les données qu'il contient. Il détermine notamment les répertoires de données, les normes et les standards applicables.

Les dispositions de mise en œuvre du référentiel général d'interopérabilité et de sécurité du système national de données de santé font l'objet d'un décret pris en Conseil des ministres.

Article 746 Conformité du système national de données de santé au référentiel d'interopérabilité et de sécurité

Le système national de données de santé et les données qui y sont conservées respectent les dispositions fixées par le référentiel général de sécurité et d'interopérabilité mentionné à l'Article 745.

Article 747 Signalement des atteintes à la sécurité et l'intégrité des systèmes d'information

Les personnes accédant aux données de santé en vertu du présent Livre signalent sans délai à l'Autorité de la cybersécurité, les incidents graves de sécurité des systèmes d'information. Les incidents de sécurité jugés significatifs sont, en outre, transmis sans délai par l'autorité nationale en charge des systèmes d'information aux autorités compétentes de l'Etat.

Sous réserve du respect des règles relatives à la protection du secret de la défense nationale, le présent article est applicable au service de santé des armées en ce qui concerne les incidents graves de sécurité des systèmes d'information concernant les activités de prévention, de diagnostic ou de soins des hôpitaux des armées.

Un décret pris en Conseil des ministres sur proposition du ministre charge de l'économie numérique et après avis de l'autorité en charge de la cybersécurité définit les catégories d'incidents de sécurité jugés significatifs et les conditions dans lesquelles ils sont traités.

Chapitre 4 : Accès et utilisation des données de santé

Article 748 Restrictions à l'accès, l'utilisation et la conservation des données du système national de données de santé

L'accès, l'utilisation et la conservation des données de santé par les citoyens, les usagers du système de santé, les professionnels de santé, les établissements de santé et leurs organisations représentatives ainsi que les organismes participant au financement de la couverture contre le risque maladie ou réalisant des traitements de données concernant la santé, les services de l'Etat, les institutions publiques compétentes en matière de santé et les organismes de presse, sont autorisés pour une durée déterminée et dans les conditions définies par le présent Chapitre et, le cas échéant, par les dispositions propres au traitement de ces données.

Article 749 Objectifs des traitements des données contenues du système national de données de santé

Un accès aux données de santé ne peut être autorisé que pour permettre des traitements soit :

1. Contribuant à une finalité mentionnée à l'Article 739 et répondant à un motif d'intérêt public ;

2. Nécessaires à l'accomplissement des missions des services de l'Etat, des établissements publics ou des organismes chargés d'une mission de service public compétents.

Les données du système national des données de santé ne peuvent être traitées pour l'une des finalités suivantes :

1. La promotion des médicaments ou de produits de santé auprès des professionnels de santé ou des établissements de santé ;

2. L'exclusion de garanties des contrats d'assurance et la modification de cotisations ou de primes d'assurance d'un individu ou d'un groupe d'individus présentant un même risque.

Article 750 Utilisations autorisées des données de santé

L'utilisation de données de santé non anonymes est soumise à autorisation de la Commission Nationale de Protection des Données à Caractère Personnel.

Article 751 Modalités d'octroi des autorisations

Les autorisations d'utilisation des données de santé non anonymes sont délivrées aux conditions édictées par l'Article 81.

Article 752 Gratuité de l'accès aux données de santé pour le secteur public

L'accès aux données de santé est gratuit pour :

1. Les traitements de données concernant la santé demandés par l'Etat ;
2. Les recherches réalisées exclusivement pour les besoins de services publics administratifs.

Chapitre 5 : Hébergement des données de santé

Article 753 Objet de l'hébergement de données de santé

L'activité d'hébergement de données de santé consiste à héberger les données de santé recueillies à l'occasion d'activités de prévention, de diagnostic, thérapeutiques, de soins ou de suivi social et médico-social :

1. Pour le compte d'une personne physique ou morale responsable de traitement, tel qu'il est défini par le Livre Préliminaire du présent Code, à l'origine de la production ou du recueil de ces données ;
2. Pour le compte du patient lui-même.

Ne constitue pas une activité d'hébergement le fait de se voir confier des données pour une courte durée par les personnes physiques ou morales à l'origine de la production ou du recueil de ces données, afin d'effectuer un traitement de saisie, de mise en forme, de matérialisation ou de dématérialisation de ces données.

Article 754 Information de la personne concernée

L'hébergement, quel qu'en soit le support, papier ou numérique, est réalisé après que la personne concernée en ait été informée.

Article 755 Droit d'opposition

La personne concernée peut s'opposer à l'hébergement de ses données de santé pour des motifs légitimes communiqués à l'hébergeur.

Article 756 Conclusion d'un contrat de prestation de services d'hébergement

La prestation d'hébergement de données de santé fait l'objet d'un contrat entre l'hébergeur et son client.

Article 757 Conditions générales de l'hébergement

L'accès aux données ayant fait l'objet d'un hébergement s'effectue selon les modalités fixées dans le contrat de prestation de services d'hébergement.

Article 758 Contenu du contrat de prestation de services d'hébergement

Le contrat de prestation de services d'hébergement contient au moins les clauses suivantes, qui peuvent être complétées par décret pris en Conseil des ministres :

1. L'indication du périmètre du certificat de conformité ou de l'agrément obtenu par l'hébergeur, ainsi que ses dates de délivrance et de renouvellement ;

2. La description des prestations réalisées, comprenant le contenu des services et résultats attendus notamment aux fins de garantir la disponibilité, l'intégrité, la confidentialité et la possibilité de contrôler les données hébergées ;

3. L'indication des lieux d'hébergement ;

4. Les mesures mises en œuvre pour garantir le respect des droits des personnes concernées par les données de santé dont notamment :

    a. les modalités d'exercice des droits de portabilité des données ;

    b. les modalités de signalement au responsable de traitement de la violation des données;

    c. les modalités de conduite des audits par le délégué à la protection des données à caractère personnel

5. La mention du référent à contacter par l'hébergeur pour le traitement des incidents ayant un impact sur les données de santé hébergées ;

6. La mention des indicateurs de qualité et de performance permettant la vérification du niveau de service annoncé, le niveau garanti, la périodicité de leur mesure, ainsi que l'existence ou l'absence de pénalités applicables au non-respect de ceux-ci ;

7. Une information sur les conditions de recours à d'éventuels prestataires techniques externes et les engagements de l'hébergeur pour que ce recours assure un niveau de protection équivalent de garantie au regard des obligations pesant sur l'hébergeur ;

8. Les modalités retenues pour encadrer les accès aux données de santé hébergées ;

9. Les obligations de l'hébergeur à l'égard de la personne pour le compte de laquelle il héberge les données de santé en cas de modifications ou d'évolutions techniques introduites par lui ou imposées par le cadre légal ou réglementaire applicable ;

10. Une information sur les garanties et les procédures mises en place par l'hébergeur permettant de couvrir toute défaillance éventuelle de sa part ;

11. La mention de l'interdiction pour l'hébergeur d'utiliser les données de santé hébergées à d'autres fins que l'exécution de l'activité d'hébergement de données de santé ;

12. Une présentation des prestations à la fin de l'hébergement, notamment en cas de perte ou de retrait de certification de l'hébergeur, et les modalités de mise en œuvre de la réversibilité de la prestation d'hébergement de données de santé ;

13. L'engagement de l'hébergeur de restituer, à la fin de la prestation, la totalité des données de santé au responsable de traitement ou au patient ;

14. L'engagement de l'hébergeur de détruire les données de santé à la fin de la prestation sans en garder de copie, après l'accord formel du responsable de traitement ou du patient.

Lorsque le responsable de traitement de données de santé ou le patient fait appel à un prestataire qui recourt lui-même à un hébergeur pour l'hébergement des données, le contrat qui lie le responsable de traitement ou le patient avec son prestataire reprend les clauses mentionnées ci-dessus telles qu'elles figurent dans le contrat liant le prestataire et l'hébergeur.

Article 759 Responsabilité de l'hébergeur

L'hébergeur est responsable de la réalisation de la prestation d'hébergement des données de santé aux conditions fixées au présent Chapitre, envers les personnes physiques ou morales pour le compte desquelles il héberge les données.

Dans les cas où la prestation d'hébergement des données de santé est sous-traitée à un tiers, le sous-traitant est responsable de la réalisation de la prestation d'hébergement, dans les conditions prévues au présent Livre, à l'égard du donneur d'ordre et à l'égard des personnes physiques ou morales pour lesquelles ces données sont hébergées, sans que cela n'affecte la responsabilité du donneur d'ordre envers les personnes pour le compte desquelles les données sont hébergées.

Article 760 Certification de l'hébergeur sur support numérique

L'hébergeur de données de santé sur support numérique est titulaire d'un certificat de conformité délivré par l'autorité nationale en charge de la cybersécurité.

S'il conserve des données dans le cadre d'un service d'archivage électronique, il est également soumis aux dispositions fixées à l'Article 460.

Article 761 Activités soumises à certification

Sont considérées comme des prestations d'hébergement soumises à certification les activités suivantes, dont la liste peut être complétée par décret pris en Conseil des ministres :

1. La mise à disposition et le maintien en condition opérationnelle des sites physiques permettant d'héberger l'infrastructure matérielle du système d'information utilisé pour le traitement des données de santé ;

2. La mise à disposition et le maintien en condition opérationnelle de l'infrastructure matérielle du système d'information utilisé pour le traitement de données de santé ;

3. La mise à disposition et le maintien en condition opérationnelle de l'infrastructure virtuelle du système d'information utilisé pour le traitement des données de santé ;

4. La mise à disposition et le maintien en condition opérationnelle de la plateforme d'hébergement d'applications du système d'information ;

5. L'administration et l'exploitation du système d'information contenant les données de santé ;

6. La sauvegarde des données de santé.

Article 762 Modalités de délivrance du certificat

Les conditions de délivrance du certificat de conformité de l'hébergeur de données de santé sur support numérique sont fixées par décret pris en Conseil des ministres sur proposition du ministère en charge de l'économie numérique.

Article 763 Retrait du certificat

Le certificat peut être retiré en cas de violation des dispositions législatives ou réglementaires relatives à l'activité d'hébergement de données de santé sur support numérique, ou de violation des prescriptions fixées par le certificat, dans les conditions prévues par décret pris en Conseil des ministres sur proposition du ministre en charge de l'économie numérique

Chapitre 6 : Reconnaissance des documents sous forme numérique contenant des données de santé

Article 764 Champ d'application

Le présent Chapitre s'applique aux documents comportant des données de santé, produits, reçus ou conservés à l'occasion d'activités de prévention, de diagnostic, thérapeutiques, de soins, de compensation d'un handicap, de prévention de perte d'autonomie, ou de suivi social et médico-social réalisées par :

1. Un professionnel de santé, un établissement ou service de santé ;
2. Un professionnel ou organisme concourant à la prévention ou aux soins dont les conditions d'exercice ou les activités sont régies par des dispositions législatives ou réglementaires spécifiques ;
3. Le service de santé des armées ;
4. Un professionnel du secteur médico-social ou social ou un établissement ou service social ou médico-social.

Article 765 Force probante du document créé sous forme numérique

Un document mentionné à l'Article 764 créé sous forme numérique a la même force probante qu'un document sur support papier lorsqu'il a été établi et conservé dans les conditions établies à l'Article 377.

Article 766 Force probante de la copie numérique

La copie numérique d'un document mentionné à l'Article 764 a la même force probante que le document original sur support papier sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité.

Article 767 Destruction des originaux des copies numériques

Lorsque une copie numérique fiable d'un document mentionné à l'Article 764 a été réalisée selon les conditions posées à l'Article 766, le document original peut être détruit avant la fin de la durée légale de conservation.

Article 768 Effets de la signature apposée sur un document sous forme numérique contenant des données de santé

La signature apposée sur un document mentionné à l'Article 764 signifie, selon le cas, que :

1. La personne prise en charge a pris acte du contenu du document et y consent ;

2. Le professionnel mentionné à l'Article 764 valide le contenu du document.

Lorsque le document sur lequel la signature est apposée est créé sur un support numérique, le procédé de signature respecte les conditions du Chapitre 3 Titre 3 du Livre Quatrième.

Article 769 Elaboration de documents réunissant des données de santé à partir de documents numériques existants

A la demande des personnes directement intéressées par ces documents, les professionnels, services, établissements et organismes mentionnés à l'Article 764 peuvent mettre en forme un document comportant des données de santé à partir d'un ou plusieurs documents numériques existants sans en modifier le sens ni le contenu, et dans le respect du secret médical et de la confidentialité des données collectées et traitées.

Le document ainsi créé est présumé fiable jusqu'à preuve du contraire lorsqu'il remplit les conditions fixées à l'Article 765.

Le document créé peut être matérialisé sur support papier.

Lorsque le document ainsi créé fait l'objet d'une obligation légale de signature, celle-ci est réputée satisfaite si le document respecte les conditions fixées à l'Article 765 et si la signature respecte les dispositions de l'Article 768.

Titre 4 Télésanté

Chapitre 1 : Télémédecine

Article 770 Définition

La télémédecine est une forme de pratique médicale à distance utilisant les technologies de l'information et de la communication. Elle met en rapport un ou plusieurs professionnels médicaux entre eux ou avec le patient et, le cas échéant, avec d'autres professionnels apportant leurs soins au patient.

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.

Article 771 Actes médicaux pouvant être réalisés à distance

Les actes médicaux pouvant être réalisés à distance sont :

1. La téléconsultation, qui permet à un professionnel médical de donner une consultation à distance à un patient ;

2. La téléexpertise, qui permet à un professionnel médical de solliciter à distance l'avis d'un ou de plusieurs professionnels médicaux sur la base des informations médicales liées à la prise en charge d'un patient ;

3. La télésurveillance médicale, qui permet à un professionnel médical d'interpréter à distance les données nécessaires au suivi médical d'un patient et, le cas échéant, de prendre des décisions relatives à la prise en charge de ce patient ;

4. La téléassistance médicale, qui permet à un professionnel médical d'assister à distance un autre professionnel médical au cours de la réalisation d'un acte ;

5. La réponse médicale apportée dans le cadre d'une aide médicale d'urgence.

Article 772 Conditions de mise en œuvre de la télémédecine

Les actes de télémédecine sont réalisés dans des conditions garantissant :

1. L'authentification des professionnels médicaux intervenant dans l'acte ;

2. L'identification du patient ;

3. L'accès des professionnels médicaux aux données médicales du patient nécessaires à la réalisation de l'acte ;

4. Le cas échéant, la formation ou la préparation du patient à l'utilisation du dispositif de télémédecine.

Article 773 Conditions de réalisation des actes de télémédecine

Les actes de télémédecine sont réalisés avec le consentement libre et éclairé du patient.

Article 774 Consignation des actes de télémédecine

Sont inscrits dans le dossier du patient tenu par chaque professionnel médical intervenant dans l'acte de télémédecine :

1. Le compte rendu de la réalisation de l'acte ;

2. Les actes et les prescriptions médicamenteuses effectués dans le cadre de l'acte de télémédecine ;

3. L'identité des professionnels médicaux participant à l'acte ;

4. La date et l'heure de l'acte ;

5. Le cas échéant, les incidents techniques survenus au cours de l'acte.

Article 775 Obligation de formation

Lorsque cela est nécessaire, le patient est formé ou préparé à l'utilisation du dispositif de télémédecine par le professionnel médical en charge de l'acte de télémédecine réalisé.

Chapitre 2 : Télésoins

Article 776 Définition

Le télésoin est une forme de pratique de soins à distance utilisant les technologies de l'information et de la communication. Il met en rapport un patient avec un ou plusieurs pharmaciens, auxiliaires médicaux ou professionnels de santé dans l'exercice de leurs compétences.

Article 777 Actes de soins pouvant être réalisés à distance

Les actes de soins pouvant être réalisés à distance, lorsqu'ils ne nécessitent pas d'interaction directe sur le patient et peuvent être réalisés par le patient lui-même ou avec l'assistance d'une tierce personne autre que le pharmacien, l'auxiliaire médical ou le professionnel de santé, sont :

1. Les soins infirmiers ;

2. Les actes de sage-femme, tels que les préparations à la naissance et à la parentalité ainsi que l'établissement d'un bilan ;

3. La téléorthophonie, qui permet de prévenir, évaluer et prendre en charge les troubles de la voix, de l'articulation, de la parole, de la compréhension du langage oral ou écrit, par des actes de rééducation ;

4. La téléergothérapie et la télépsychomotricité, qui permettent de prévenir et de réduire les situations de handicap d'un patient en étudiant, concevant et aménageant son environnement pour le rendre plus accessible et sécurisé ;

5. La télékinésithérapie, qui permet de renforcer, maintenir ou rétablir les capacités fonctionnelles et motrices d'un patient ;

6. La téléorthoptie, qui permet de dépister, analyser et traiter les troubles visuels moteurs, sensoriels et fonctionnels ;

7. La télépodologie et la télépédicure, qui permettent de diagnostiquer des affections du pied ou d'assister un patient dans des actes de rééducation du pied après une intervention chirurgicale;

8. La télépharmacie, qui permet d'accompagner un patient sous traitement médicamenteux ou de réaliser un bilan thérapeutique ;

9. La télédiététique, qui permet d'apporter une expertise en nutrition et en alimentation à un patient.

Article 778 Conditions de mise en œuvre des télésoins

Les actes de télésoin sont réalisés dans des conditions garantissant :

5. L'authentification des pharmaciens, auxiliaires médicaux ou professionnels de santé intervenant dans l'acte ;

6. L'identification du patient ;

7. L'accès des pharmaciens, auxiliaires médicaux ou professionnels de santé, aux données médicales du patient nécessaires à la réalisation de l'acte ;

8. Le cas échéant, la formation ou la préparation du patient à l'utilisation du dispositif de télésoin.

Article 779 Conditions de réalisation des actes de télésoin

Les actes de télésoin sont réalisés avec le consentement libre et éclairé du patient.

Article 780 Consignation des actes de télésoin

Sont inscrits dans le dossier du patient tenu par chaque pharmacien, auxiliaire médical ou professionnel de santé intervenant dans l'acte de télésoin :

1. Le compte rendu de la réalisation de l'acte ;

2. Les actes et les prescriptions médicamenteuses effectués dans le cadre de l'acte de télésoin ;

3. L'identité des pharmaciens, auxiliaires médicaux ou professionnels de santé participant à l'acte;

4. La date et l'heure de l'acte ;

5. Le cas échéant, les incidents techniques survenus au cours de l'acte.

Article 781 Obligation de formation

Lorsque cela est nécessaire, le patient est formé ou préparé à l'utilisation du dispositif de télésoin par le pharmacien, l'auxiliaire médical ou le professionnel de santé en charge de l'acte de télésoin réalisé.

Titre 5 Interopérabilité des systèmes de paiement mobile

Chapitre unique : Cadre d'interopérabilité des systèmes de paiement mobile

Article 782 Mise en place du cadre d'interopérabilité des systèmes de paiement mobile

Sans préjudice de toute disposition fixée par la Banque Centrale de Djibouti, les systèmes de paiement mobile reposent sur le principe d'interopérabilité.

Article 783 Services de communication permettant d'effectuer des paiements mobiles

Un décret pris en Conseil des ministres après avis de l'Autorité de régulation, établira, si nécessaire, les conditions d'accès du service de communication utilisé pour effectuer des paiementsmobiles.

Livre Huitième : Dispositions modificatives, transitoires et finales

Chapitre premier : Dispositions modificatives et transitoires

Article 784 Mise en conformité des activités de traitement de données à caractère personnel, y compris des données de santé à caractère personnel et aux fins de la prospection directe

À compter de l'entrée en vigueur de la présente loi, les traitements de données à caractère personnel doivent être mis en conformité avec les prescriptions du Livre Premier et, le cas échéant, faire l'objet des formalités préalable requises, dans un délai de deux (2) ans pour les traitements effectués pour le compte de l'État, d'une personne morale de droit public ou d'une personne morale de droit privé gérant un service public, et dans un délai d'un (1) an pour les autres traitements.

Article 785 Nomination du directeur général de l'Autorité de régulation

Les services de l'Autorité de régulation Multisectorielle de Djibouti sont dirigés par un Directeur général nommé par Décret pris en conseil de ministre sur proposition de la Présidence. Le mandat du Directeur général est de trois (3) ans renouvelable une fois.

Article 786 Licences, autorisations et autorisations d'utilisation de fréquences radioélectriques existantes

Le Ministère en charge des communications électroniques sur avis de l'Autorité de régulation s'agissant des licences, et l'Autorité de régulation s'agissant des autorisations, sont en charge de la mise en conformité des licences et autorisations dans les trois (03) mois suivant la date d'entrée en vigueur de la présente loi.

Article 787 Mise en conformité des activités de communications électroniques

A compter de l'entrée en vigueur de la présente loi, toute personne se livrant à une activité soumise aux dispositions du Livre Deuxième et n'étant pas titulaire d'une autorisation, licence, d'un agrément ou permis de toute nature, est tenue de se conformer à ces dispositions et de demander toute licence, autorisation, agrément, décision d'attribution de fréquences radioélectriques ou autre autorisation ou permis de toute nature ou de procéder à toute déclaration requis pour la continuation de son activité dans un délai de six (6) mois à compter de l'entrée en vigueur de la présente loi. Si l'activité est continuée à défaut d'avoir réalisé les formalités ou présenté les demandes nécessaires à l'issue de ce délai, l'intéressé sera passible des peines prévues au Chapitre 4 du Titre 9 du Livre Deuxième.

Article 788 Contrat conclu par échange de courriers électroniques

En complément de l'article 1270 du Code civil, lorsqu'il est conclu par voie électronique, le contrat n'est valable que si le destinataire de l'offre a eu la possibilité de vérifier le détail de sa commande et son prix total et de corriger d'éventuelles erreurs avant de confirmer celle-ci pour exprimer son acceptation définitive. Toutefois cette obligation n'est pas applicable aux contrats conclus exclusivement par échange de courriers électroniques.

L'auteur de l'offre doit accuser réception sans délai injustifié, par voie électronique, de la commande qui lui a été adressée. Toutefois cette obligation n'est pas applicable aux contrats conclus exclusivement par échange de courriers électroniques.

La commande, la confirmation de l'acceptation de l'offre et l'accusé de réception sont considérés comme reçus lorsque les parties auxquelles ils sont adressés peuvent y avoir accès.

Article 789 Etablissement et conservation d'un écrit sous forme électronique pour la validité d'un contrat

En complément de l'article 1241 du Code civil, lorsqu'un écrit est exigé pour la validité d'un contrat, que ce soit sous signature privée ou par acte authentique, il peut être établi et conservé sous forme électronique, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir non seulement l'intégrité mais encore le lien entre la signature électronique et l'acte auquel elle s'attache.

Une signature électronique a le même effet juridique qu'une signature manuscrite selon les conditions et modalités prévues par la loi. »

Article 790 Présomption de fiabilité d'un procédé de signature électronique

En complément de l'article 1596 du Code civil, la signature nécessaire à la perfection d'un acte juridique identifie son auteur. Elle manifeste son consentement aux obligations qui découlent de cet acte. Quand elle est apposée par un officier public, elle confère l'authenticité à l'acte. Lorsqu'elle est électronique, elle a le même effet juridique qu'une signature manuscrite selon les conditions et modalités prévues par la loi. »

Article 791 Mise en conformité des activités de fourniture de moyens et de prestations de cryptologie

A compter de l'entrée en vigueur de la présente loi, toute personne se livrant à une activité soumise aux dispositions du Livre Troisième est tenue de se conformer à ces dispositions et

de procéder à toute déclaration ou de demander toute autorisation ou permis de toute nature requis pour la continuation de son activité dans un délai de six (6) mois à compter de l'entrée en vigueur de la présente loi, au plus tard.

Chapitre 2 : Dispositions finales

Article 792 Mesures d'application du Livre Premier

Des décrets pris en Conseil des ministres sur proposition du ministère en charge de l'économie numérique et après avis de la Commission Nationale de Protection des Données à Caractère Personnel fixent les modalités d'application des dispositions du Livre Premier.

Article 793 Mesures d'application du Livre Deuxième

Sans préjudice des modalités particulières prévues à cet effet, des décrets pris en Conseil des ministres sur proposition du ministre en charge des communications électroniques, après avis de l'Autorité de régulation multisectorielle de Djibouti fixent les modalités d'application des dispositions du Livre Deuxième.

Article 794 Mesures d'application du Livre Quatrième

Sans préjudice des modalités particulières prévues à cet effet, des décrets pris en Conseil des ministres sur proposition du ministère en charge de l'économie numérique après avis de l'Autorité de régulation, fixent les modalités d'application des dispositions du Livre Quatrième.

Un arrêté pris en conseil des ministres sur proposition du Ministère charge de l'économie numérique fixe le montant des redevances dues à l'Organe en charge de la certification racine par les prestataires de services de confiance qualifiés pour l'octroi du statut qualifié.

Article 795 Mesures d'application du Livre Cinquième

Sans préjudice des modalités particulières prévues à cet effet, des décrets pris en Conseil des ministres fixent les modalités d'application des dispositions du Livre Cinquième. Ceux relatifs au Titre 1 du Livre Cinquième sont pris après avis de l'Autorité de régulation multisectorielle de Djibouti exceptés ceux relatifs au Titre 1 Chapitre 4 du Livre Cinquième, qui sont pris après avis de l'Autorité de régulation multisectorielle de Djibouti et de la Commission Nationale de Protection des Données à Caractère Personnel.

Article 796 Mesures d'application du Livre Sixième

Le Président de la République, après avis du ministère en charge de l'économie numérique, détermine, le cas échéant, les autorités compétentes ainsi que les conditions d'application des dispositions du Livre Sixième.

Sans préjudice des modalités particulières prévues à cet effet, des décrets pris en Conseil des ministres sur proposition du ministère en charge de l'économie numérique fixent les modalités d'application des dispositions du Livre Sixième.

Article 797 Mesures d'application du Livre Septième

Des décrets pris en Conseil des ministres sur proposition du ministère en charge de l'économie numérique, et le cas échéant, après avis de la Commission nationale de protection des données personnelles, après avis du ministre de la Santé, ou en concertation avec l'autorité nationale en charge des systèmes d'information l'Autorité de la cybersécurité, fixent les modalités d'application des dispositions du Livre Septième.

Article 798 Abrogation des textes antérieurs à la présente loi.

Toutes les dispositions antérieures contraires à la présente loi sont abrogées, notamment la loi n° 80/AN/04/5ème L du 24 octobre 2004 portant réforme du secteur des technologies de l'information et de la communication,