PROJET DE LOI PORTANT CODE DU NUMERIQUE EN REPUBLIQUE DEMOCRATIQUE DU CONGO

(Ministère du Numérique)

EXPOSÉ DES MOTIFS

La République Démocratique du Congo s'est engagée dans la voie d'un programme qui vise à assurer sa transformation numérique, à travers la digitalisation de son administration publique et de tous les autres secteurs de la vie nationale tant publics que privés.

Dans le cadre de ce programme, le numérique constitue un levier d'intégration, de bonne gouvernance, de croissance économique et du progrès social du pays, et à ce titre, l'adoption d'un nouveau cadre légal et règlementaire sur le numérique est une priorité.

La loi n° 20/017 du 25 novembre 2020 relative aux télécommunications et aux technologies de l'information et de la communication, abrogeant la loi-cadre n° 013/2002 du 16 octobre 2002 sur les télécommunications en République Démocratique du Congo, avait pour objectif notamment de prendre en compte et de règlementer les nouvelles technologies de l'information et de la communication.

Force est cependant de constater que la loi n° 20/017 du 25 novembre 2020 précitée, à l'instar de celle qu'elle a abrogée, a mis l'accent sur le secteur des télécommunications et n'a pris en compte que très partiellement les situations complètement inédites, notamment les nouvelles activités ou services numériques non identifiés, la protection des données à caractère personnel, la cybersécurité et la cybercriminalité.

Ladite loi n'a pas règlementé certaines autres matières relevant du numérique, notamment le commerce électronique, la valeur juridique des écrits et outils électroniques ainsi que leur création, certification et archivage, d'une part, et n'a pas prévu la création d'un organisme indépendant chargé de la protection des données à caractère personnel et d'autres agences, notamment celles chargées de sécuriser les systèmes d'informations ainsi que de la lutte contre la cybercriminalité, d'autre part.

A cet effet, l'adoption d'un nouveau cadre juridique a pour but de combler les lacunes en matière du numérique et de rechercher un point d'équilibre entre, d'une part, les principes de liberté sur le web, notamment la liberté d'expression, d'information, de réunion et d'opinion et, d'autre part, la protection de la vie privée ainsi que la protection de l'ordre public.

La présente loi portant code du numérique établit une démarcation entre le secteur des télécommunications et celui du numérique, ce dernier mettant l'accent sur la production, la collecte, le traitement, la circulation et l'échange, le stockage et la sécurité des données.

La présente loi, qui trouve son fondement à l'article 122, points 1, 6, 8 et à l'article 123, point 8 de la Constitution, définit le régime juridique applicable aux activités et services numériques, aux écrits et outils électroniques, aux prestataires des services de confiance, au commerce et aux échanges électroniques, à la protection des données à caractère personnel ainsi qu'à la cybersécurité et à la cybercriminalité et en fixe le cadre institutionnel.

Elle apporte également les innovations ci-après :

- la consécration de la notion des activités et de celle de fournisseurs de services numériques notamment les prestataires de service de confiance, de même que la définition des régimes juridiques qui s'y rapportent ;
- la mise en place d'un régime juridique applicable au commerce électronique et aux échanges d'informations par voie électronique au sein de l'administration publique ;
- l'érection des principes de l'identification digitale, de la signature électronique et du cachet électronique ainsi que les circonstances de son admission ;
- la mise en place des institutions appropriées pour la protection des systèmes d'informations, la protection des données à caractère personnel et l'Autorité de certification électronique électronique ;
- la consécration des règles de procédure en matière de lutte contre la cybercriminalité.

Hormis le livre préliminaire consacré à l'objet de la loi, à son champ d'application et aux définitions, la présente loi est subdivisée en sept livres suivants :

- Livre I : Des activités et services numériques ;
- Livre II : Des écrits et outils électroniques ;
- Livre III : Des prestataires de services de Confiance ;
- Livre IV : Du commerce et des échanges électroniques ;
- Livre V : De la protection des données à caractère personnel ;
- Livre VI : De la cybersécurité et de la cybercriminalité ;
- Livre VII : Des dispositions diverses, transitoires et finales.

Telle est l'économie de la présente loi.

Loi

L'Assemblée Nationale et le Sénat ont adopté ;

Le Président de la République promulgue la Loi dont la teneur suit :

LIVRE PRÉLIMINAIRE : DE L'OBJET, DU CHAMP D'APPLICATION ET DES DÉFINITIONS

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

Article 1.

Le présent Livre définit le régime juridique et fixe le cadre institutionnel applicable aux activités et services numériques, écrits et outils électroniques, prestataires des services de confiance, commerce et échanges électroniques, à la protection des données à caractère personnel ainsi qu'à la cybersécurité et cybercriminalité.

Article 2.

Sans préjudice des dispositions légales et réglementaires en vigueur, la présente loi s'applique :

1. aux activités et services numériques ;
2. aux écrits et outils électroniques ;
3. aux prestataires de services de confiance ;
4. aux commerce et échanges électroniques ;
5. à la protection des données à caractère personnel ;
6. à la cybersécurité et à la cybercriminalité ;
7. aux dispositions diverses, transitoires et finales.

CHAPITRE II : DES DÉFINITIONS

Article 3.

Au sens du présent Livre, on entend par :

1. **Abonné** : toute personne physique ou morale qui bénéficie, moyennant paiement, d'un service de communications numériques en vertu d'un contrat, conformément aux modalités établies par l'opérateur ;
2. **Accès/Service universel** : offre minimale au public, sur l'ensemble du territoire national, de services de communications numériques à un prix abordable et, ce, dans le respect des principes d'égalité, de continuité et d'universalité ;
3. **Accès** : (i) toute pénétration directe ou indirecte dans l'intégralité ou une partie quelconque d'un système numérique. La pénétration indirecte s'entend de l'accès intervenant via un réseau de communications numériques de quelle que nature que ce soit. Le mode de communication utilisé pour ledit accès est non pertinent ; (ii) toute 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 numériques ou de fournir des services de communications numériques, y compris les prestations associées telle que la colocalisation ;

4. **Accès illégal** : accès sans droit à un système numérique ou tout comportement sans droit susceptible de mettre en péril ou mettant en péril la confidentialité, l'intégrité et la disponibilité de données numériques ;
5. **Adresse** : physique et/ou électronique
6. **ANSSI** : Agence Nationale de Sécurité des Systèmes d'Information ;
7. **ADN** : Agence de Développement du Numérique ;
8. **APD** : Autorité de Protection des Données ;
9. **Archivage numérique** : organisation et conservation des archives par voie du numérique
10. **Archivage** : opération consistant à organiser et conserver des archives aux fins d'une utilisation ultérieure, que cette conservation soit administrative ou historique ;
11. **Archives** : Documents, quelle que soit leurs dates, leurs formats et leurs supports, produits ou reçus et délibérément conservés par toute personne, physique ou morale, publique ou privée ;
12. **ARPTC** : Autorité de Régulation des Postes et des Télécommunications du Congo ;
13. **Assignation d'une fréquence ou d'un canal radioélectrique** : toute autorisation accordée à un opérateur d'utiliser une ou plusieurs fréquences selon des conditions spécifiées ;
14. **Atteinte à l'intégrité d'un système** : tout acte qui entrave l'usage légitime du système numérique
15. **Atteinte à l'intégrité des données** : tout acte susceptible de mettre ou mettant en péril la sécurité des données numériques ;
16. **Attentat à la pudeur** : consiste dans le fait de commettre un acte impudique sur une personne contre sa volonté, soit que le défaut de consentement résulte de la violence physique ou morale exercée à son égard, soit qu'il résulte de tout autre moyen de contrainte ou de surprise employé pour atteindre le but recherché par l'auteur de l'action ;
17. **Attribution d'une bande de fréquence** : inscription dans le tableau d'attribution des bandes de fréquences, d'une bande de fréquences déterminée, aux fins de son utilisation par un ou plusieurs services ;
18. **Autorisation** : acte administratif de l'Autorité de régulation qui confère à un opérateur un ensemble de droits et d'obligations spécifiques en vertu desquels cet opérateur est fondé à exercer certaines activités de communications électroniques conformément aux dispositions de la présente loi ;
19. **Autorité compétente** : autorité désignée par voie réglementaire en charge de superviser les activités du numérique conformément à la présente loi ;

20. **Autorité de contrôle** : autorité administrative chargée de veiller au respect, sur le territoire national, de la présente loi ;
21. **Autorité de protection des données** : autorité administrative chargée de veiller à ce que les traitements des données à caractère personnel soient mis en œuvre conformément à la présente loi ;
22. **Autorité de régulation** : organisme public administratif chargé de réguler les activités du numérique en République Démocratique du Congo ;
23. **Boucle locale et sous-boucle locale** : circuit physique qui relie les points de terminaison d'un réseau de communications électroniques dans les locaux des abonnés au répartiteur principal ou à toute autre installation équivalente du réseau de communications numériques d'un opérateur ;
24. **Cachet électronique** : données électroniques, jointes ou associées logiquement à d'autres données électroniques afin de garantir l'originalité et l'intégrité de ces dernières
25. **Cachet électronique avancé** : cachet électronique qui satisfait aux exigences de la présente loi ;
26. **Cachet électronique qualifié** : cachet électronique avancé créé à l'aide d'un dispositif de création de cachet électronique qualifié et qui repose sur un certificat qualifié de cachet électronique ;
27. **Cahier des charges** : document intégrant les conditions techniques et les modalités d'exploitation imposées à tout opérateur ou fournisseur de services postaux ou de services de communications numériques ouverts au public ;
28. **Catégories particulières de données** : données génétiques, données liées à des mineurs, données relatives aux infractions, aux condamnations pénales ou aux mesures de sûreté, données biométriques ainsi que, pour autant qu'elles soient traitées pour ce qu'elles révèlent ou contiennent, les données à caractère personnel qui révèlent l'origine raciale ou ethnique, la filiation, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, le sexe ainsi que le traitement des données relatives à la santé et à la vie sexuelle ;
29. **CERT** (Computer Emergency Response Team) **ou CSIRT** : organisme officiel chargé d'assurer des services de prévention des risques et d'assistance au traitement d'incidents. Des centres d'alerte et de réaction aux attaques informatiques destinés aux entreprises et/ou aux administrations, dont les informations sont généralement accessibles à tous ;
30. **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 ;

31. **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 ;
32. **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 ou le pseudonyme de cette personne ;
33. **Certificat qualifié d'authentification de site Internet** : attestation délivrée par un prestataire de services de confiance qualifié et qui satisfait aux exigences fixées par la présente loi ;
34. **Certificat qualifié de cachet électronique** : acte délivré par un prestataire de services de confiance qualifié et qui satisfait aux exigences fixées par voie réglementaire ;
35. **Certificat qualifié de signature électronique** : acte délivré par un prestataire de services de confiance qualifié et qui satisfait aux exigences fixées par voie réglementaire ;
36. **Client :** toute personne physique ou morale qui, pour la satisfaction d'un besoin, recourt aux opérations d'achats des biens ou de prestation des services auprès d'un vendeur, d'un fournisseur ou d'un prestataire de services.
37. **Code** : loi portant code du numérique ;
38. **Code de conduite** : ensemble de dispositions qui servent de repère aux opérateurs du système numérique ;
39. **Code pénal** : ensemble de dispositions répressives en vigueur en République Démocratique du Congo ;
40. **Collecte en temps réel** : rassemblement des preuves contenues dans des communications numériques au moment même de leur transmission ;
41. **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 ;
42. **Commerce électronique** : activité commerciale par laquelle une personne propose ou assure par voie numérique, moyennant paiement d'un prix, la fourniture de biens ou de services ;
43. **Communication électronique** : toute émission, toute transmission et toute réception de signes, de signaux, d'écrits, d'images, de sons ou d'informations de toute nature par fil, fibre optique, radioélectricité ou autres systèmes électromagnétiques ;
44. **Confidentialité** : état de sécurité permettant de garantir le secret des informations et ressources stockées dans les réseaux et systèmes de communication numérique, systèmes d'information et/ou des équipements terminaux, afin d'en prévenir la

divulgation non autorisée d'informations à des tiers, par la lecture, l'écoute, la copie illicite d'origine intentionnelle ou accidentelle durant leur stockage, traitement ou transfert ;

45. **Consentement de la personne concernée** : toute manifestation de volonté expresse, non équivoque, libre, spécifique et informée par laquelle la personne concernée ou son représentant légal, judiciaire ou conventionnel accepte par une déclaration ou par un acte positif clair que les données à caractère personnel le concernant fassent l'objet d'un traitement ;
46. **Consentement** : manifestation de volonté expresse et non équivoque par laquelle la personne concernée accepte que ses données à caractère personnel fassent l'objet d'un traitement ;
47. **Conservation des données** : sauvegarde des données en l'état dans lequel elles se trouvent, en les protégeant contre tout ce qui pourrait en modifier ou détériorer la qualité ou l'état actuel ;
48. **Consommateur** : tout utilisateur du numérique ;
49. **Contenu numérique** : ensemble de données logées dans le système numérique
50. **Contrat de vente en ligne** : le contrat de vente par Internet ;
51. **Coût net** : différence entre les coûts d'investissement et d'exploitation nécessaires à la fourniture de l'accès/service universel et les recettes pertinentes ; les recettes pertinentes étant les recettes directes et indirectes induites par l'accès/service universel
52. **Créateur de cachet** : personne qui crée des cachets électroniques ;
53. **Cryptologie** : ensemble des pratiques visant la protection et la sécurité des données numériques notamment pour la confidentialité, l'authentification, l'intégrité et la non répudiation ;
54. **Cryptographie** : art d'écrire en chiffres, en caractères secrets ;
55. **CSAC** : Conseil Supérieur de l'Audiovisuel et de la Communication.
56. **Cybercriminalité :** Ensemble des infractions pénales spécifiques liées aux technologies de l'information et de la communication telles que définies par la présente loi, ainsi que celles dont la commission est facilitée ou liée à l'utilisation de ces technologies.
57. **Cyberdéfense** : ensemble de moyens physiques, virtuels et organisationnels mis en place par un pays pour détecter et contrer les cyberattaques dont la cible et la finalité sont liées à la défense nationale.
58. **Cybersécurité** : ensemble des moyens qui permettent d'assurer la protection et l'intégrité des données numériques ainsi que leur commercialisation ;
59. **Déclaration** : acte préalable à toute activité émanant d'un opérateur ou d'un fournisseur des services de télécommunications et de technologies de l'information de la communication, qui n'oblige pas l'entreprise concernée à obtenir une décision explicite de l'Autorité de régulation avant d'exercer les droits découlant de cet acte.

60. **Dégroupage de la boucle-locale** : opération technique qui permet aux opérateurs tiers d'accéder à la boucle locale du réseau ouvert au public. Elle est soit, en partie, par le biais de découpage partiel, soit en totalité, par le biais du découpage total.
61. **Destinataire :** toute personne habilitée à recevoir la communication des données autre que la personne concernée, le responsable du traitement du sous-traitant et les personnes qui, en raison de leurs fonctions, sont chargées de traiter les données.
62. **Diffusion** : action consistant à transmettre des données numériques à autrui ;
63. **Digitalisation** : Opération de numérisation, consistant à transformer un signal, une grandeur physique, en sa représentation numérique ;
64. **Dispositif** : matériel ainsi que solutions basées sur des logiciels dans l'intention de commettre l'une des infractions visées au Livre II de la présente loi ;
65. **Documents administratifs** : tout document reçu, produit ou détenu par un organisme public dans le cadre de ses missions ou de ses attributions, notamment les correspondances, faits, opinions, avis, mémorandums, données, statistiques, livres, dessins, plans, cartes, diagrammes, photographies et enregistrements audiovisuels ou numériques ;
66. **Donnée personnelle** : toute information enregistrée, exclusive à une personne identifiée dans le système numérique relative à un particulier identifié ou identifiable, directement ou indirectement, grâce à un identifiant ou à un ou plusieurs éléments propres à son identité. Par exemple : nom, photo, adresse, identifiant en ligne, numéro de carte d'identité, données de localisation, données de santé, profil culturel ou social, etc. ;
67. **Données à caractère personnel** : (i) pour les personnes physiques : toute information relative à une personne physique identifiée ou identifiable directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments, propres à son identité physique, physiologique, génétique, psychique, culturelle, sociale ou économique ; (ii) pour les personnes morales : toute information relative à une personne morale identifiée ou identifiable directement par plusieurs éléments propres à son identité. Par exemple : la dénomination ou raison sociale, le siège social, ses statuts et son RCCM, etc. ;
68. **Données afférentes à la création de signature** : données uniques telles que des codes ou des clés cryptographiques privées, que le signataire utilise pour créer une signature électronique sécurisée ;
69. **Données biométriques** : toutes les données relatives aux caractéristiques physiq0210ues, physiologiques ou comportementales d'une personne physique qui permettent son identification unique, telles que des images faciales ou des données dactyloscopiques ;
70. **Données concernant la santé** : toute information concernant l'état physique et mental d'une personne concernée, y compris les données génétiques et la prestation de

services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne ;

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

72. **Données de création de cachet électronique** : données uniques qui sont utilisées par le créateur du cachet électronique pour créer un cachet électronique ;

73. **Données génétiques** : toute donnée concernant les caractères héréditaires d'un individu ou d'un groupe d'individus apparentés.

74. **Données informatiques** : toute représentation de faits, d'informations, de concepts, de codes ou d'instructions lisibles par une machine, sous une forme qui se prête à un traitement informatique y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction ;

75. **Données relatives au contenu** : contenu informatif de la communication, c'est-à-dire le sens de la communication, ou le message ou l'information véhiculés par la communication. Il s'agit de tout ce qui est transmis dans le cadre de la communication en dehors des données relatives au trafic ;

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

77. **Données relatives aux abonnés** : toute information, sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de services et se rapportant aux abonnés de ses services, autres que des données relatives au trafic ou au contenu, et permettant d'établir (i) le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service ; (ii) l'identité, l'adresse postale ou géographique, le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de services ; (iii) toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de services ;

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

79. **Droits de passage** : servitude permettant de mettre en place des infrastructures et équipements nécessaires à l'exploitation d'un réseau ou d'une fourniture d'un service numérique ;

80. **Effacer** : action de détruire des données numériques ;
81. **Émissions électromagnétiques** : émissions pouvant provenir d'un ordinateur en fonctionnement. Elles ne sont pas considérées comme des données informatiques au sens des définitions, ci-dessus. Cependant, des données peuvent être reconstituées à partir de telles émissions ;
82. **Entraver** : actions de porter atteinte au bon fonctionnement du système numérique. Elle résulte de l'introduction, du transfert, de l'endommagement, de l'effacement, de l'altération ou de la suppression de données informatiques. En relation avec un système informatique, l'entrave peut consister, sans s'y limiter, à :
    a. couper l'alimentation électrique d'un système informatique ;
    b. provoquer des interférences électromagnétiques dans un système informatique
    c. corrompre un système informatique par quelque moyen que ce soit ;
    d. introduire, transmettre, endommager, effacer, détériorer, altérer ou supprimer des données informatiques
83. **Équipement terminal** : tout équipement destiné à être connecté directement ou indirectement à un point de terminaison d'un réseau en vue de la transmission, de la réception, du traitement ou de la visualisation d'informations ;
84. **Escroquerie :** définie par l'article 98 du code pénal, livre II ;
85. **Établissement principal :** lieu de l'administration centrale ;
86. **Exigences essentielles** : ensemble de règles requises pour garantir :
87. **Exploitant d'infrastructures alternatives** : toute personne qui détient, exploite ou assure la gestion d'infrastructures ou de droits pouvant supporter ou contribuer à supporter des réseaux du numérique ;
88. **Fichier** : répertoire structuré des données numériques, que ce répertoire soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique ;
89. **Flux transfrontalier de données à caractère personnel** : ensemble de données à caractère personnel transmises, d'un pays étranger à la République Démocratique du Congo, à une période déterminée, par voie du numérique ;
90. **Fournisseur d'accès** : toute personne physique ou morale qui fournit à un utilisateur un service dans un réseau de communication ou un accès à un réseau de communication de transmission des données numériques soit un accès à un réseau numérique ;
91. **Fournisseur de cache** : toute personne physique ou morale fournissant un service de transmission électronique de données par stockage automatique, intermédiaire et temporaire des informations, dans le but de rendre plus efficace la transmission des informations ;
92. **Fournisseur de liens hypertextes** : toute personne physique ou morale qui fournit un ou plusieurs liens hypertexte ;

93. **Fournisseur de services en ligne** : toute personne physique ou morale qui ouvre l'opportunité à d'autres d'utiliser les services du numérique ;
94. **Fournisseur en position dominante :** tout fournisseur disposant sur un marché de services ou d'un groupe de services d'une puissance significative, équivalent au moins à 25 % du volume ou de la valeur de ce marché peut être déclaré dominant) ;
95. **Fréquence radioélectrique** : nombre de cycles par seconde à partir duquel un courant électrique analogique change de sens ; elle est généralement mesurée en hertz (Hz). Un hertz est égal à un cycle par seconde ;
96. **Gestion du spectre des fréquences** : ensemble des actions administratives et techniques visant à assurer une utilisation rationnelle et efficace du spectre des fréquences radioélectriques par les utilisateurs ;
97. **Gouvernance numérique** : gestion basée sur la technologie et l'outil du numérique ;
98. **Hébergeur** : toute personne physique ou morale qui fournit un service de transmission électronique de données en stockant les informations fournies par l'utilisateur du service
99. **Horodatage électronique** : opération visant à associer à un fichier sa date et son heure de création ou de réception (au sens du guide pratique de la dématérialisation des marchés publics) ;
100. **Horodatage électronique qualifié** : horodatage électronique qui satisfait aux exigences fixées par la présente loi ;
101. **INACO** : Institut National des Archives du Congo ;
102. **Identification électronique** : processus consistant à utiliser des données d'identification personnelle sous une forme électronique représentant de manière univoque une personne physique ou morale ;
103. **Identité** : le caractère permanent et fondamental de quelqu'un, d'un groupe, qui fait son individualité, sa singularité ;
104. **Identité numérique :** ensemble de contenus univoques publiés sur internet qui permettent de définir un individu ;
105. **Information** : élément de connaissance, exprimé sous forme écrite, visuel, sonore ou numérique susceptible d'être représenté à l'aide des conventions pour être utilisé, conservé, traité ou communiqué.
106. **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 ;
107. **Infrastructure alternative** : toute installation ou ensemble d'installations pouvant assurer ou contribuer à assurer la transmission et/ou l'acheminement de signaux de communications électroniques ;

108. **Infrastructure essentielle** : toute infrastructure de communications numérique actives ou passives ou toute infrastructure alternative 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 ;

109. **Infrastructure sensible ou critique** : point, système ou partie de celui-ci, situé sur le territoire de la République Démocratique du Congo et qui est indispensable au maintien des fonctions vitales de la société, de la santé, de la sûreté, de la sécurité et du bien-être économique ou social des citoyens, comme les centrales électriques, les réseaux de transport et les réseaux publics, et dont l'arrêt ou la destruction aurait un impact significatif sur la République Démocratique du Congo du fait de la défaillance de ces fonctions ;

110. **Installation de communications électroniques** : tous équipements, appareils, câbles, éléments 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 ;

111. **Intégrité** : état de sécurité assurant qu'un réseau de communications électroniques, système d'information ou équipement terminal qui est demeuré intact et que les ressources et informations qui y sont stockées n'ont pas été altérées, modifiées ou détruites, d'une façon intentionnelle ou accidentelle, de manière à assurer leur exactitude, leur fiabilité et leur pérennité ;

112. **Interception** : acquisition, prise de connaissance, saisie ou copie du contenu ou d'une partie du contenu de toute communication, y compris les données relatives au contenu, les données informatiques, les données relatives au trafic, lors de transmissions non publiques par le biais de moyens techniques. L'interception comprend, sans que cette liste soit limitative, l'écoute, le contrôle ou la surveillance du contenu des communications et l'obtention du contenu des données, soit directement, au moyen de l'accès aux systèmes d'information et de leur utilisation, soit indirectement, au moyen de l'utilisation de dispositifs d'écoute électroniques ou de dispositifs d'écoute par des moyens techniques ;

113. **Interconnexion** : liaison physique et logique des réseaux de communications numérique électroniques utilisés par la même entreprise ou une entreprise différente, afin de permettre aux utilisateurs d'une entreprise de communiquer avec les utilisateurs de la même entreprise ou d'une autre, ou bien d'accéder aux services fournis par une autre entreprise ; ces services peuvent être fournis par les parties concernées ou par d'autres parties qui ont accès au réseau ; l'interconnexion constitue un type particulier d'accès mis en œuvre entre opérateurs de réseaux publics ou privés. Les prestations

d'interconnexion comprennent également les prestations associées telle que la co-localisation ;

114. **Interconnexion des fichiers des données à caractère personnel** : tout mécanisme de connexion consistant en la mise en relation de données traitées pour une finalité déterminée avec d'autres données traitées pour des finalités identiques ou non, ou liées par un ou plusieurs responsables de traitement ;
115. **Intermédiaire de commerce** : profession des métiers de la vente tels que : agent commercial, commissionnaire, courtier, apporteur d'affaires, etc. ;
116. **Interopérabilité des équipements terminaux** : aptitude d'un équipement à fonctionner, d'une part, avec le réseau auquel il est connecté et, d'autre part, avec l'ensemble des autres équipements terminaux connecté à un réseau et qui permettent d'accéder à un même service ;
117. **Introduction de données** : manipulations à l'entrée du système de données inexactes, manipulations de programmes ou autres ingérences dans le traitement des données ;
118. **Itinérance nationale ou national roaming** : toute forme de partage d'infrastructures actives, permettant aux abonnés d'un opérateur mobile d'avoir accès au réseau et aux services offerts par un autre opérateur mobile offrant ladite itinérance dans une zone non couverte par le réseau nominal desdits abonnés ;
119. **Large bande** : réseau capable de transmettre des signaux à un débit élevé. En opposition à un réseau bande de base qui utilise un seul canal de transmission, un réseau large bande utilise plusieurs canaux de transmission. Un canal de transmission étant égal à 64 Kbps, tout réseau transmettant à plus de 128 Kbps est un réseau large bande. Les technologies peuvent être par câble, ondes hertziennes ou satellitaires. Les technologies par câbles comprennent la paire de cuivre, le câble électrique, la fibre optique et une technologie hybride câble fibre optique ;
120. **Licence** : toute autorisation accordée par arrêté du Ministre sectoriel, portant approbation d'un cahier des charges, à toute personne qui répond aux conditions prévues dans la présente loi et qui s'engage à en respecter les dispositions ; elle définit les modalités et les conditions suivant lesquelles le titulaire de la licence est autorisé à exercer son activité de communications électroniques et fixe les droits et obligations de celui-ci ;
121. **Lien hypertexte** : caractéristique ou propriété d'un élément tel qu'un symbole, un mot, une phrase ou une image qui contient des informations sur une autre source et qui renvoie et affiche un autre document lorsqu'elle est exécutée ;
122. **Limitation du traitement** : marquage de données à caractère personnel conservées, en vue de limiter leur traitement futur ;
123. **Liste de confiance :** ensemble d'éléments essentiels pour établir la confiance entre les acteurs du marché numérique en permettant aux utilisateurs de déterminer le statut

qualifié et l'historique du statut des prestataires de services de confiance et de leurs services.

124. **Logiciels** : un ensemble de programmes qui vont être exécutés par la machine pour réaliser une tâche.

125. **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 une contrepartie financière est exigée ;

126. **Market place** : toute plateforme qui met en relation des acheteurs et des vendeurs sur internet ;

127. **Matériel raciste et xénophobe** : tout matériel 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 ;

128. **Mémoire** : dispositif électronique numérique qui sert à stocker des données ;

129. **Mesure de sécurité** : tous dispositifs ou programmes informatiques spécialisés à l'aide desquels l'accès à un système informatique est limité ou interdit pour certaines catégories d'utilisateurs ;

130. **Mise à disposition** : action consistant à mettre, notamment, des dispositifs, matériels, et informations en ligne pour qu'ils soient utilisés par autrui ;

131. **Monétique** : ensemble des techniques informatiques et électroniques appliquées à la réalisation des transactions bancaires ;

132. **Monnaie électronique** : est légalement une monnaie stockée sur des mémoires électroniques de façon indépendante d'un compte bancaire ;

133. **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 ;

134. **Moyen de stockage de données informatiques** : tout objet ou support à partir duquel des informations peuvent être reproduites, avec ou sans l'aide d'un autre objet ou dispositif ;

135. **Moyens techniques** : dispositifs techniques connectés aux lignes de transmission ainsi que dispositifs de collecte et d'enregistrement de communications sans fil. Ils peuvent entre autres consister en des logiciels, mots d'accès et codes ;

136. **MVNO *« Mobile Virtual Network Operator »* ou Opérateur de réseau mobile virtuel** : tout opérateur de téléphonie mobile ne possédant pas d'autorisation d'utilisation de fréquences radioélectriques ni d'infrastructures de radiocommunications qui contracte

avec les opérateurs de radiocommunication afin de fournir aux utilisateurs des services de communications électroniques mobiles ;

137. **Neutralité technologique** : obligation pour la législation numérique d'être non-discriminatoire entre les opérateurs du secteur ;
138. **Numérique** : c'est la donnée, les outils et services de son exploitation ainsi que l'ensemble du processus de son traitement ;
139. **Numéro** : toute chaîne de chiffres indiquant de façon univoque le point de terminaison du réseau public. Il contient l'information nécessaire à acheminer jusqu'au point de terminaison. Il 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 ;
140. **Opérateur** : toute personne physique ou morale exploitant un réseau de communications numériques ou fournissant un service de communications numériques. Les opérateurs sont impérativement soumis au régime de la licence, de l'autorisation ou de l'entrée libre avec ou sans déclaration ;
141. **Opérateur de radiocommunication** : opérateur exploitant un réseau numérique utilisant les fréquences de radioélectrique soumises à une autorisation préalable ;
142. **Opérateur dominant** : tout opérateur disposant sur un marché de services ou d'un groupe de services une puissance significative, équivalent au moins à 25 % du volume ou de la valeur de ce marché ;
143. **Opérateur fournissant un accès à internet** : tout opérateur offrant un service permettant un accès à internet à des personnes physiques ou morales, à titre lucratif ou non ;
144. **Opérateur national** : tout opérateur titulaire d'une licence ou ayant réalisé une déclaration en République Démocratique du Congo, ou bénéficiant du droit d'exploitation d'un réseau numérique ou de fournir des services numériques ;
145. **Opérateur non national** : tout opérateur exerçant ses activités à l'étranger, ne bénéficiant d'aucune licence en République Démocratique du Congo ;
146. **Organe de Contrôle** : autorité chargée de contrôler les activités des prestataires de services de confiance, conformément à la présente loi ;
147. **Organisme d'évaluation de la conformité** : tout organisme qui effectue des opérations d'évaluation de la conformité, comme l'étalonnage, les essais, la certification et l'inspection ;
148. **Organisme public** : l'État, les collectivités territoriales et les personnes de droit public chargées d'une mission de service public ;
149. **Paiement électronique** : moyen permettant d'effectuer des transactions commerciales ou l'échange de biens ou des services sur l'internet ;

150. **Personne concernée** : toute personne physique qui fait l'objet d'un traitement des données à caractère personnel et qui est identifiée ou identifiable ;
151. **Piratage informatique** : tout accès sans autorisation à un système informatique ;
152. **Plainte** : toute requête adressée à l'Autorité compétente pour revendiquer et faire reconnaître un droit que l'auteur estime posséder ou pour manifester une insatisfaction contre un opérateur ;
153. **Plan national de numérotation** : plan organisant la ressource constituée par l'ensemble des numéros et permettant notamment d'identifier les points de terminaison fixes ou mobiles des réseaux et services téléphoniques, d'acheminer les appels et d'accéder à des ressources internes aux réseaux ;
154. **Point de terminaison** : point de connexion physique répondant à des spécifications techniques, nécessaires pour avoir accès à un réseau de communications numérique et communiquer efficacement par son intermédiaire ;
155. **Portabilité des numéros** : possibilité pour un utilisateur d'utiliser le même numéro d'abonnement, indépendamment de l'opérateur chez lequel il est abonné et même dans le cas où il change d'opérateur ;
156. **Possession** : détention ou jouissance d'une chose ou d'un droit qu'une personne tient ou qu'elle exerce par elle-même, ou par une autre qui la tient ou qui l'exerce en son nom ;
157. **Prestataire de service de confiance** : personne physique ou morale qui fournit un ou plusieurs services de confiance ;
158. **Prestataire de service de confiance qualifié** : prestataire de services de confiance qui fournit un ou plusieurs services de confiance ayant obtenu le statut qualifié ;
159. **Prestataire de services électroniques de confiance qualifié** : celui doit vérifier l'identité d'une personne physique ou morale pour pouvoir émettre un certificat électronique en sa faveur ;
160. **Prestataire des services de paiement** : entreprise agréée pour offrir des services de paiement ;
161. **Prestataire des services** : société dont la fonction consiste à fournir aux commerçants en ligne des services pour qu'ils soient en mesure de traiter les paiements électroniques. Autrement-dit, il est le lien entre commerçant et la banque, qui permet de faciliter à la fois l'autorisation de générer des commandes d'achat et de percevoir le paiement ;
162. **Professionnel** : toute personne physique ou morale qui 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 ;
163. **Professionnel des soins de santé** : toute personne définie comme telle par la réglementation en vigueur en la matière ;

164. **Profilage** : toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique ;
165. **Programme informatique** : ensemble ordonné d'instructions pouvant être exécutées par l'ordinateur pour obtenir le résultat attendu ;
166. **Prospection directe** : tout envoi de message destiné à promouvoir, directement ou indirectement, des biens, des services ou l'image d'une personne vendant des biens ou fournissant des services ;
167. **Pseudonymisation** : 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 ;
168. **Radiocommunications** : communications réalisées à l'aide d'ondes radioélectriques
169. **RCCM** : Registre du Commerce et du Crédit Mobilier ;
170. **Règlement des radiocommunications** : manuel publié par l'UIT contenant les recommandations relatives à la radiocommunication
171. **Représentant du responsable de traitement** : toute personne physique ou morale établit de manière stable sur le territoire du pays, qui se substitue au responsable de traitement dans l'accomplissement des obligations prévues par la présente loi
172. **Réseau de communications él**ectroniques : toute installation ou tout ensemble d'installations de transport ou de diffusion ainsi que, le cas échéant, les autres moyens assurant l'acheminement de communication numérique, notamment ceux de commutation et de routage ;
173. **Réseau indépendant** : tout réseau du numérique réservé à un usage privé ou partagé.
174. **Réseau interne** : tout réseau indépendant entièrement établi sur une même propriété, sans emprunter ni le domaine public y compris hertzien, ni l'espace atmosphérique ni une propriété tierce ;
175. **Réseau ouvert au public** : tout réseau du numérique établi et/ou exploité pour fournir des services de communications électroniques au public, y compris des capacités nationales et internationales ;
176. **Réseau, installation et équipement terminal radioélectriques** : réseau, installation et équipement terminal utilisant des fréquences hertziennes pour la propagation des ondes

électromagnétiques en espace ; au nombre des réseaux radioélectriques figurent notamment les réseaux utilisant les capacités des satellites ;

177. **Réseau** : ensemble connecté des systèmes informatiques, quel que soit leur mode de connexion, qui peuvent être reliées à la terre, sans fil ou les deux ;

178. **Responsable du traitement** : personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel ; lorsque les finalités et les moyens du traitement sont déterminés par des dispositions législatives ou réglementaires nationales, le responsable du traitement ou les critères spécifiques pour le désigner peuvent être fixés par le droit national ;

179. **Schéma d'identification numérique** : système pour l'identification numérique en vertu duquel des moyens d'identification électronique sont délivrés à des personnes physiques ou morales, ou à des personnes physiques représentant des personnes morales ;

180. **Sécurité de données numériques** : confidentialité, intégrité et disponibilité de données informatiques ;

181. **Sélection du transporteur** : mécanisme de choix d'un opérateur devant acheminer une partie ou l'intégralité de ses appels ;

182. **Service d'envoi recommandé électronique qualifié** : service d'envoi recommandé électronique qui satisfait aux exigences fixées par le présent Code ;

183. **Service d'envoi recommandé numérique** : service qui permet de transmettre des données entre tiers, par voie numérique, en fournissant des preuves concernant le traitement des données transmises ;

184. **Service de confiance** : service électronique normalement fourni contre rémunération et qui consiste :

    a. en la création, la vérification et la validation de signatures électroniques, de cachets électroniques ou d'horodatages électroniques, de services d'envoi recommandé électronique et de certificats relatifs à ces services ;
    b. en la création, la vérification et la validation de certificats pour l'authentification de site Internet ;
    c. en la conservation de signature électronique, de cachets électroniques ou des certificats relatifs à ces services.

185. **Service de confiance qualifié** : service de confiance qui satisfait aux exigences de l'article 298 du présent Code ;

186. **Service de radiocommunication** : tout service impliquant la transmission, l'émission ou la réception de fréquences radioélectriques se propageant dans l'espace sans guide artificiel à des fins spécifiques de communications numérique ;

187. **Service ou activité numérique** : activité ou service permettant à l'utilisateur ou consommateur de créer, de traiter des données sous forme numérique, ou d'y accéder

de même que tout service permettant le partage ou toute autre interaction avec les données sous forme numérique qui sont téléversées, mises en ligne ou crées par les autres utilisateurs de ce service ;

188. **Service téléphonique au public** : exploitation commerciale pour le public qui consiste dans le transfert direct de la voix et l'image en temps réel au départ et à destination de réseaux de communication ouverts au public entre utilisateurs fixes ou mobiles ;
189. **Services à valeur ajoutée** : tout service du numérique qui répondent à de nouveaux besoins spécifiques de communication ;
190. **Services de communications électroniques** : toutes prestations incluant l'émission, la transmission ou la réception de signes, de signaux, d'écrits, d'images, de sons ou d'informations de toute nature ou une combinaison de ces fonctions ;
191. **Servitudes** : obligations grevant les propriétés privées au profit du domaine public ou dans un but d'intérêt général. Elles sont instituées notamment, en vue de la protection des centres radio électriques d'émission et de réception contre les obstacles physiques.
192. **Signal numérique** : signal au moyen duquel les informations sont représentées par un nombre fini de valeurs discrètes bien déterminées
193. **Signataire** : toute personne qui détient un dispositif de création de signature et qui agit soit pour son propre compte, soit pour celui d'une entité ou d'une personne physique ou morale qu'elle représente ;
194. **Signature électronique** : mécanisme permettant de garantir l'intégrité d'un document électronique et d'en authentifier l'auteur ;
195. **Signature électronique qualifiée** : signature électronique répondant aux exigences de l'article 261 du présent Code ;
196. **Soldat numérique** ou cyberdéfenseur : (i) logiciel ou robot informatique résilient doté d'intelligence artificielle capable de sécuriser le cyberespace congolais contre des attaques cybernétiques, d'analyser et anticiper des situations critiques d'intrusions et de cyber-espionnage. (ii) logiciel résilient doté de capacité d'analyse des comportements cybernétiques afin de lutter contre la fraude informationnelle, la propagation des malveillances dans des infrastructures critiques essentielles et des systèmes d'information stratégiques de l'État
197. **Sous-traitant** (ou entreprise sous-traitante) : personne physique ou morale dont l'activité, à titre habituel, temporaire ou occasionnel, est liée, par un contrat ou une convention, à la réalisation de l'activité principale ou à l'exécution d'un contrat d'une entreprise principale ; la personne physique ou morale, l'autorité publique, le service public ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement et sous ses instructions
198. **Sous-traitance** : activité ou opération effectuée par une entreprise dite sous-traitance, pour le compte d'une entreprise dite entreprise principale et qui concourt à la réalisation

de l'activité principale de cette entreprise, ou à l'exécution d'une ou de plusieurs prestations d'un contrat de l'entreprise principale ;

199. **Souveraineté numérique** : droit de véto qu'un pays dispose sur les données numériques de toute la nation y compris sur les données numériques de ses citoyens en tant que actifs dans l'univers numérique ;
200. **Spectre de fréquences radioélectriques** : désigne l'ensemble de bandes de fréquences radioélectriques ;
201. **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 en un emplacement donné ;
202. **Support durable** : tout instrument permettant à l'emprunteur de conserver les informations qui lui sont adressées personnellement, d'une marnière qui permet de s'y reporter aisément à l'avenir et qui permet la reproduction identique desdites informations ;
203. **Système informatique** : Un système informatique est un dispositif composé de matériels et de logiciels, conçus pour le traitement automatisé des données numériques
204. **Technologies de l'Information et de la Communication (TIC) :** toute technique utilisée dans le traitement et la transmission des informations, principalement l'informatique, l'internet et les communications électroniques. Elles désignent aussi le secteur d'activité économique de technologies de l'information et de la communication numérique ;
205. **Tiers** : personne physique ou morale, l'autorité publique, le service ou tout autre organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont habilitées à traiter les données ;
206. **Traitement** : toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés entièrement ou partiellement automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, 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 ;
207. **Traitement automatique ou automatisé de données informatiques** : ensemble des opérations réalisées en totalité ou en partie par des moyens automatisés, relatifs à la collecte, l'enregistrement, l'élaboration, la modification, la conservation, la destruction, l'application d'opérations logiques et/ou arithmétiques l'édition des données et d'une façon générale, leur exploitation sans intervention humaine directe ;
208. **Transmission** : tous les transferts de données, par téléphone, télécopie, courriel ou transfert de fichiers ;
209. **UIT** : Union Internationale des Télécommunications ;

210. **Utilisateur** : toute personne physique ou morale qui utilise ou demande à bénéficier d'un réseau et/ou service du numérique ;
211. **Utilisateur final** : consommateur des services numériques ;
212. **Vendeur en ligne :** personne physique ou morale possédant des biens ou ayant une capacité à produire des services, se départit de ces biens ou fournit des services moyennant rémunération en utilisant pour cette activité des supports électroniques et/ou numérique.
213. **Violation de données à caractère personnel** : violation de la sécurité entraînant de manière accidentelle ou illicite la destruction, la perte, l'altération, la divulgation ou la consultation non autorisées de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données, l'intrusion à de telles données.

LIVRE PREMIER : DES ACTIVITÉS ET SERVICES NUMÉRIQUES

TITRE I : DE L'OBJET ET DU CHAMP D'APPLICATION

Article 4.

Sans préjudice des dispositions particulières, le présent livre régit les activités et services numériques exercés à partir ou à destination du territoire de la République Démocratique du Congo, par toute personne physique ou morale, quels que soient son statut juridique, sa nationalité ou celle des détenteurs de son capital social ou de ses dirigeants, du lieu de son siège social ou de son établissement principal.

Article 5.

Sont exclus du champ d'application du présent Livre :

1. les activités et services numériques exercés pour les besoins de la sécurité publique et de la défense nationale ;
2. la réglementation et la régulation des télécommunications ;
3. la règlementation et régulation du secteur de l'audiovisuel.

TITRE II : DES ACTIVITES ET SERVICES NUMERIQUES

CHAPITRE I : DU CADRE INSTITUTIONNEL

Article 6.

Le cadre institutionnel du secteur des activités et services numériques comprend :

1. le Ministre ayant le numérique dans ses attributions ;
2. l'Autorité de régulation ;
3. l'Agence de Développement du Numérique ;
4. le Conseil national du numérique.

Section I : Du Ministre

Article 7.

Sans préjudice d'autres textes législatifs et réglementaires en vigueur, le Ministre ayant le numérique dans ses attributions a pour missions de :

1. concevoir, proposer et mettre en œuvre la politique du gouvernement dans le secteur du numérique ;
2. assurer, dans les limites de ses compétences, la réglementation, la promotion et le suivi des activités et services du secteur du numérique ;
3. élaborer le plan national de numérisation intégrée de l'Administration et des services publics et piloter sa mise en œuvre, en collaboration avec les ministères sectoriels ;

4. promouvoir, en collaboration avec les ministères sectoriels, la transformation vers l'économie numérique et le développement de l'innovation nationale ;
5. arrêter les règlements d'administration et de police relatifs aux activités et services numériques et fixer les droits, taxes et redevances y afférents ;
6. concevoir et initier des programmes d'investissements d'avenir dans le secteur du numérique ;
7. élaborer et coordonner, en collaboration avec les ministères sectoriels et services de l'Etat, les cahiers des charges techniques de mise en œuvre des programmes et projets nationaux dans le secteur du numérique ;
8. concevoir les outils de planification des programmes et des projets nationaux dans le secteur du numérique ;
9. assurer la mise en place et la gestion des infrastructures et équipements numériques, notamment des data centers publics ;
10. représenter et défendre les intérêts du pays auprès des organisations sous-régionales, régionales et internationales de même qu'assurer l'application des traités et accords internationaux conclus par l'Etat dans le secteur du numérique ;
11. traiter de toutes questions relatives à la promotion et à la diffusion du numérique, à la gouvernance de l'Internet, aux infrastructures et équipements numériques, aux services, contenus et usages numériques, à la sécurité des échanges, des réseaux et des systèmes d'information.

Section II : De l'Autorité de régulation

Article 8.

L'Autorité de régulation a notamment pour missions de :

1. réguler les activités et services numériques ;
2. veiller à l'équité des prix et à la qualité des services rendus aux utilisateurs ;
3. définir les principes d'interopérabilité des services numériques ;
4. protéger sur le marché du numérique les intérêts des utilisateurs et des fournisseurs de services numériques en veillant à l'existence et à la promotion d'une concurrence effective et loyale, et prendre toutes les mesures nécessaires aux fins de rétablir la concurrence au profit des usagers ;
5. assurer la police des activités et des services du secteur du numérique ;
6. veiller au respect de la concurrence dans le secteur du numérique et trancher les litiges y afférents.

Article 9.

Les missions de régulation des activités et services du numérique sont assurées par l'Autorité de régulation prévue par la loi n° 20/017 du 25 novembre 2020 relative aux télécommunications et technologies de l'information et de la communication sous la tutelle conjointe du Ministre ayant le numérique dans ses attributions.

Section III : De l'Agence de Développement du Numérique

Article 10.

Il est créé, par Décret du Premier Ministre délibéré en Conseil des Ministres, une Autorité de certification électronique des services et équipements numériques fournis à l'Etat et de promotion du numérique dénommé Agence de Développement du Numérique, « ADN » en sigle.

L'ADN est un établissement public à caractère technique, placé sous la tutelle du Ministre ayant le numérique dans ses attributions.

Il est doté de la personnalité juridique, jouit de l'autonomie de gestion et dispose d'un patrimoine propre.

Article 11.

L'ADN a pour d'assurer le rôle de l'Autorité de certification électronique, de promouvoir et de contribuer à la mise en œuvre de la politique du gouvernement dans le secteur du numérique.

Sans préjudice des compétences spécifiques dévolues à certains services publics particuliers, l'ADN est chargée de :

1. délivrer les certifications électroniques en tant qu'Autorité de certification électronique ;
2. contribuer à la recherche, à la mobilisation et à la canalisation des financements nécessaires à la réalisation des projets de développement du numérique ;
3. participer à la réduction de la fracture numérique ;
4. participer à la coordination des projets numériques sectoriels, la mutualisation des ressources des projets numériques publics ;
5. élaborer et gérer le plan national des adresses IP publiques ;
6. veiller à l'intégrité des informations du domaine-pays Internet ;
7. contribuer à la promotion de l'industrie numérique locale, de l'innovation technologique, des centres d'excellence et de recherche ;
8. produire des rapports périodiques sur l'état général de l'écosystème numérique national ;
9. assurer la promotion des activités et services numériques dans les milieux ruraux et péri-urbains ne présentant pas d'intérêt pour les opérateurs économiques du secteur.

Une quotité du fonds de service universel sera affectée au fonctionnement de l'Autorité de certification électronique et à la promotion des activités et services numériques.

Section IV : Du Conseil National du Numérique

Article 12.

Il est créé, par Décret du Premier ministre, un organique consultatif dénommé : Conseil National du Numérique en République Démocratique du Congo, en sigle « CNN », ci-après dénommé « Le Conseil national ».

Il comprend l'ensemble des acteurs du secteur du numérique, à savoir le Gouvernement et ses services, le secteur privé ainsi que la société civile.

Le Conseil national est placé sous la tutelle du Ministre ayant le Numérique dans ses attributions.

Article 13.

Sans préjudice des attributions de l'Agence du Développement Numérique, le Conseil national a notamment pour mission de :

- servir de cadre de concertation et d'évaluation des projets du Gouvernement dans le secteur du numérique ;
- Etudier et donner des avis au Gouvernement sur les questions en relation avec le numérique ;
- Evaluer les politiques sectorielles et les initiatives des investissements numériques ;
- Proposer et présenter au Ministre du numérique des initiatives sectorielles ainsi que les entraves d'exécution des projets à caractère numérique.

CHAPITRE II : DES DROITS ET PRINCIPES GENERAUX APPLICABLES AUX FOURNISSEURS DES SERVICES NUMERIQUES

Article 14.

Sans préjudice des dispositions particulières, les activités et services numériques sont soumis aux principes ci-après :

- Egalité de traitement ;
- Transparence ;
- Non-discrimination ;
- Libre concurrence ;
- Neutralité technologique.

Les activités et services numériques s'exercent librement, dans le respect des dispositions légales et réglementaires applicables en République Démocratique du Congo.

Article 15.

Les fournisseurs des services numériques jouissent de mêmes droits et sont soumis aux mêmes obligations conformément aux dispositions du présent Code.

Les principes d'égalité de traitement, de non-discrimination des fournisseurs des services numériques et de transparence des procédures s'imposent à toute autorité administrative, notamment à l'Autorité de régulation et à l'Agence de Développement du Numérique, y compris dans le cadre des procédures applicables aux différents régimes juridiques concernant les activités et services numériques en République Démocratique du Congo.

Sont interdites les dispositions qui, par leurs exigences particulières, écartent certaines catégories de fournisseurs des services numériques en se fondant sur des considérations contraires à la loi.

Les autorités administratives s'assurent que l'accès à un régime par un fournisseur respecte les règles de libre concurrence.

Les fournisseurs des services numériques garantissent également la neutralité de traitement des données au regard des messages transmis et des informations qui y sont liées.

Article 16.

Les fournisseurs des services numériques intervenant sous un même régime juridique jouissent, dans les mêmes conditions, de mêmes droits et sont soumis aux mêmes obligations prévues à ce régime.

Sans préjudice des dispositions de l'alinéa précédent, les conditions d'exercice dépendent du respect des conditions matérielles ou techniques préalablement fixées par l'Autorité de régulation.

Ces conditions doivent être compatibles avec les règles nationales en matière de concurrence.

Article 17.

L'Autorité de régulation veille à l'application, en toutes circonstances, du principe de neutralité technologique.

Le principe de neutralité technologique s'entend comme l'obligation générale de non-discrimination légale, réglementaire, institutionnelle ou autre des technologies au regard des services fournis.

Article 18.

Les activités et services numériques menés sur le territoire national par les représentations diplomatiques, les institutions étrangères et les organismes jouissant de la personnalité juridique

de droit international, sont exercés conformément aux traités et accords internationaux ratifiés par la République Démocratique du Congo.

Sous réserve des dispositions particulières des traités et accords internationaux ratifiés par la République Démocratique du Congo, les activités et services numériques des représentations diplomatiques, des institutions étrangères et des organismes jouissant de la personnalité juridique de droit international sont soumis aux dispositions du présent Code.

Article 19.

Pour la réalisation des travaux nécessaires à l'exploitation et à l'extension de leurs activités, les fournisseurs des services numériques sont tenus de respecter l'ensemble des dispositions législatives et réglementaires en vigueur, notamment les prescriptions en matière d'aménagement du territoire et de protection de l'environnement.

Article 20.

Les accords entre fournisseurs des services numériques et utilisateurs sur les conditions commerciales et techniques, telles que les prix, les volumes de données ou le débit et toutes pratiques commerciales mises en œuvre par les fournisseurs des services numériques, ne peuvent limiter les droits acquis des utilisateurs en matière de fourniture des services.

Article 21.

L'Autorité de régulation veille à la qualité et à la disponibilité permanente des services numériques fournis.

Elle peut imposer des exigences concernant des caractéristiques techniques, des exigences minimales de qualité du service et d'autres mesures adaptées et nécessaires à un ou plusieurs fournisseurs des services numériques.

A la demande de l'Autorité de régulation, les fournisseurs des services numériques mettent à sa disposition toute information relative à leurs obligations et communiquent ces informations dans les délais et selon le degré de précision exigés par elle.

CHAPITRE III : DES OBLIGATIONS DES FOURNISSEURS DES SERVICES NUMERIQUES

Article 22.

Tout fournisseur des services numériques a l'obligation de :

1. rendre disponibles à tout utilisateur les infrastructures et services numériques ouverts au public qu'il fournit ;
2. s'assurer que les frais, les tarifs, les pratiques et les classifications sont justes, raisonnables et disponibles de façon transparente ;
3. fournir des services efficaces et conformes aux normes reconnues au plan national, international ou fixées par l'Autorité de régulation ;

4. publier par tout moyen d'information de masse et sans délais, les prévisions d'interruption de services, notamment pour des raisons d'installation, de réparation ou de changement d'équipement ;
5. établir un mécanisme efficace de traitement des réclamations et de résolution expéditive des incidents ;
6. veiller au respect des règles relatives à la protection des données à caractère personnel.

Article 23.

Sauf décision prise en application d'une loi ou d'un règlement en vigueur, toute personne physique ou morale qui remplit les conditions contractuelles et financières proposées par un fournisseur des services numériques ne peut se voir refuser la fourniture de ces services, s'il en a formulé la demande.

Le fournisseur des services numériques peut néanmoins exiger de l'utilisateur demandeur desdits services un dépôt de garantie dont le montant est préalablement fixé et publié de manière transparente et non-discriminatoire.

Tout utilisateur d'un service numérique qui respecte les conditions contractuelles et financières souscrites ne peut subir l'interruption de fourniture des services, à moins qu'il en fasse la demande expresse, sauf en cas de force majeure ou pour des raisons de sécurité publique.

Article 24.

Les informations transparentes et actualisées relatives à l'ensemble des services proposés, aux tarifs pratiqués ainsi qu'aux conditions générales de vente et/ou de services, sont régulièrement publiées et mises à la disposition des utilisateurs par les fournisseurs des services numériques dans leurs points de vente et par tout autre moyen de publicité.

L'Autorité de régulation précise, par une décision, les délais de publication, la forme et le contenu des informations et documents à publier.

Article 25.

Tout fournisseur des services numériques élabore des contrats types pour la fourniture des services aux utilisateurs.

L'Autorité de régulation précise les dispositions que doivent contenir les contrats conclus avec les utilisateurs.

Article 26.

Aucun fournisseur des services numériques ne peut limiter le droit de l'utilisateur de jouir pleinement des services auxquels il a souscrit.

Article 27.

Les fournisseurs de services numériques ne peuvent unilatéralement modifier les termes d'un contrat en cours qui les lie aux utilisateurs que :

1. pour des raisons indiquées dans les termes du contrat et conformément à ce dernier ;
2. sur base d'un changement de la législation ou d'une décision de l'Autorité de régulation en application d'une disposition légale ou réglementaire.

Tout projet de modification des conditions contractuelles de fourniture d'un service numérique est communiqué par le fournisseur dudit service aux utilisateurs par écrit ou sur un autre support durable mis à la disposition de ces derniers au moins un mois avant son entrée en vigueur, assorti de l'information selon laquelle les utilisateurs peuvent, tant qu'ils n'ont pas expressément acceptés les nouvelles conditions, résilier le contrat sans pénalité de résiliation et sans droit au dédommagement, jusque dans un délai de deux mois après l'entrée en vigueur de la modification.

La modification ne prend effet qu'à l'issue de ce délai de deux mois.

Article 28.

Les fournisseurs des services numériques ont l'obligation de garantir l'accès aux services d'urgence conformément aux règles applicables et dans les conditions précisées par l'Autorité de régulation.

L'accès à ces services ne peut souffrir d'aucune limitation. Toutefois, cette obligation n'est opérable que dans les zones couvertes par les services fournis.

Article 29.

Les fournisseurs des services numériques ne peuvent utiliser leurs infrastructures ou sciemment en permettre l'utilisation à des fins contraires aux dispositions légales et règlementaires en vigueur.

Ils sont tenus de prendre toutes mesures appropriées pour s'assurer que leurs infrastructures ne soient pas utilisées à des fins illégales ou frauduleuses.

Article 30.

Sauf en cas de réquisitions judiciaires, les fournisseurs des services numériques sont tenus aux exigences de confidentialité des données qu'ils traitent conformément aux dispositions du Livre V du présent Code.

CHAPITRE IV : DU RÉGIME JURIDIQUE DES ACTIVITES ET SERVICES NUMERIQUES

Section I : Des dispositions générales

Article 31.

Sans préjudice des dispositions applicables aux sociétés commerciales, nul ne peut exercer une activité dans le secteur du numérique sans se soumettre à l'un des régimes juridiques prévus par le présent Code.

Article 32.

L'exercice des activités et services numériques est soumis au régime d'autorisation, de déclaration ou de certification, selon les cas, conformément aux modalités et conditions d'octroi fixées dans le présent Code et par arrêté du Ministre ayant le numérique dans ses attributions.

L'instruction des demandes d'autorisation ou de déclaration, ainsi que l'élaboration du cahier de charges relève de l'Autorité de régulation.

Section II : De l'autorisation

Article 33.

Sont soumis au régime d'autorisation :

1. les fournisseurs des services numériques de confiance qualifiée ;
2. les fournisseurs des services numériques essentiels ;
3. les fournisseurs des services d'hébergement d'applications financières ;
4. les opérateurs de télécommunication offrant ou désirant offrir des services numériques de masse et possédant déjà des infrastructures en République Démocratique du Congo soumis à un des régimes juridiques prévus par la loi régissant le secteur des télécommunications.

Cette liste n'étant pas exhaustive, le Ministre ayant le numérique dans ses attributions dispose du pouvoir de la compléter, l'Autorité de régulation entendue par avis écrit.

Article 34.

L'autorisation est délivrée par le Ministre ayant le Numérique dans ses attributions après avis de l'Autorité de régulation.

Section III : De la déclaration

Article 35.

Sont soumis au régime de déclaration :

1. les fournisseurs de services numériques construisant des centres de données ;
2. les fournisseurs des services numériques d'hébergement d'applications et de contenus ;
3. les fournisseurs de services numériques de copies tampon ou serveurs cache des contenus des données ou médias d'autres fournisseurs ;
4. les opérateurs de points d'échange Internet ;
5. les fournisseurs des contenus en ligne ;
6. les cybercafés et hot spot ;
7. les services à valeurs ajoutées numériques des opérateurs des télécommunications ;
8. les systèmes de télésurveillance ou de vidéosurveillance dans les espaces privés fermés ou ouverts au public.

Cette liste n'étant pas exhaustive, le Ministre ayant le numérique dans ses attributions dispose du pouvoir de la compléter, l'Autorité de régulation entendue par avis écrit.

Article 36.

La déclaration est faite auprès de l'Autorité de régulation qui tient un registre public.

L'Autorité de régulation prend acte de toute déclaration par la délivrance d'un certificat d'agrément et en informe le Ministre ayant le numérique dans ses attributions.

CHAPITRE V : DE LA CERTIFICATION DES SERVICES NUMERIQUES FOURNIS A L'ETAT

Article 37.

La certification atteste que les services et équipements numériques fournis à l'Etat sont conformes aux normes, standards et bonnes pratiques en la matière.

Sont soumis à la certification :

1. les fournisseurs des services numériques à l'État ou à toute autre entité publique;
2. les fournisseurs des services numériques à un service public ou à une entreprise du portefeuille de l'État.

Cette liste n'étant pas exhaustive, le Ministre ayant le numérique dans ses attributions dispose du pouvoir de la compléter, l'Autorité de certification électronique entendue par avis écrit.

Un arrêté du Ministre ayant le numérique dans ses attributions fixe les conditions et modalités d'octroi de la certification.

Article 38.

La certification est délivrée par le Ministre ayant le numérique dans ses attributions après avis de l'Autorité de certification électronique.

TITRE III : DE LA RÉGULATION DES FOURNISSEURS EN POSITION DOMINANTE

Article 39.

L'Autorité de régulation assure l'équilibre du marché du secteur du numérique, en veillant à une concurrence loyale et effective.

Les fournisseurs en position dominante, notamment les plates-formes en ligne, sont soumis à des obligations spécifiques en matière d'équité.

L'Autorité de régulation assure une mission de prévention et de répression à l'encontre des fournisseurs en position dominante après analyse de l'état et de l'évolution prévisible des aspects de la concurrence du marché.

Article 40.

La position dominante du fournisseur est appréciée sur base des critères ci-après :

1. sa capacité à influencer le marché ;
2. son chiffre d'affaires par rapport à la taille du marché ;
3. le contrôle qu'il exerce sur les moyens d'accès à l'utilisateur final ;
4. sa capacité à agir indépendamment de ses concurrents, de ses clients et des consommateurs.

Article 41.

Un arrêté du Ministre ayant le numérique dans ses attributions fixe les modalités d'application des dispositions relatives à la régulation des fournisseurs en position dominante.

TITRE IV : DE LA GESTION DES RESSOURCES RARES

CHAPITRE I : DES DISPOSITIONS GÉNÉRALES

Article 42.

Les ressources rares sont :

1) les adresses IP publiques ;
2) le nom du domaine Internet national.

Un arrêté du Ministre ayant le numérique dans ses attributions fixe les politiques et règles de gestion des ressources rares en République Démocratique du Congo.

CHAPITRE II : DE L'ADRESSAGE ET NOMS DE DOMAINES

Section I : De la gestion du plan national d'adressage

Article 43.

L'établissement du plan national d'adressage et la maîtrise de l'identification de toutes les ressources nationales d'adressage sont de la compétence de l'Autorité de certification électronique.

L'Autorité de certification électronique formule des demandes auprès du registre international des adresses IP et des blocs de ressources d'adresses à mettre à la disposition des acteurs de l'écosystème numérique congolais.

Les adresses ne peuvent devenir la propriété des demandeurs ou des utilisateurs finaux.

Section II : Du nom de domaine Pays

Article 44.

Le domaine pays Internet relève du domaine de l'Etat.

La gestion du domaine pays Internet est confiée à l'Autorité de certification électronique.

En application de l'alinéa précédent, un arrêté du Ministre ayant le numérique dans ses attributions fixe les modalités de gestion administrative, technique et commerciale des noms des domaines constituant le domaine Pays.

Article 45.

Les noms de domaine Pays sont attribués pour une durée limitée et renouvelable.

L'enregistrement des noms de domaine Pays s'effectue sur base des déclarations faites par le demandeur et sous sa responsabilité.

TITRE V : DU RÈGLEMENT DES DIFFÉRENDS

CHAPITRE I : DES COMPÉTENCES DE L'AUTORITÉ DE RÉGULATION

Article 46.

Sans préjudice de la compétence consultative reconnue à l'Autorité de régulation, elle connait des différends tant entre fournisseurs des services numériques qu'entre utilisateurs et fournisseurs des services numériques.

Elle est saisie à la demande de la partie la plus diligente ou par saisine d'office.

Article 47.

L'Autorité de régulation peut être saisie d'un différend entre un fournisseur des activités et services numériques nationaux et un fournisseur des activités et services numériques étrangers, à la diligence de l'une des parties.

Dans ce cas, elle saisit l'Autorité de régulation du pays du fournisseur des activités et services numériques mis en cause.

Article 48.

Lorsqu'elle est saisie ou informée par une Autorité de régulation compétente d'un autre État dans le cadre d'un différend entre un fournisseur des activités et services numériques nationaux et un fournisseur des activités et services numériques étrangers, l'Autorité de régulation coordonne ses efforts avec elle dans le règlement du différend.

Article 49.

L'Autorité de régulation est saisie par voie de requête lorsque la demande émane de l'une des parties au litige ou procède par voie d'instruction lorsqu'elle se saisit d'office.

Elle se saisit d'office lorsque le litige est de nature à porter atteinte à la continuité des services dans le secteur du numérique.

Article 50.

L'Autorité de régulation est tenue de procéder à une tentative de règlement amiable en cas de contentieux entre fournisseurs des services numériques ou entre ces derniers et les utilisateurs.

Elle instruit les demandes dans un délai qui ne peut dépasser un mois à dater de sa saisine.

Les décisions de l'Autorité de régulation doivent être motivées et sont susceptibles de recours administratifs devant le Conseil d'Etat conformément aux dispositions de la loi organique n° 16-027 du 18 octobre 2016 portant organisation, compétence et fonctionnement des juridictions de l'ordre administratif.

TITRE VI : DES MESURES, SANCTIONS ET DE LA PRESCRIPTION

CHAPITRE I : DES MESURES ET SANCTIONS ADMINISTRATIVES

Article 51.

Lorsqu'un fournisseur des activités et services numériques titulaire d'une autorisation ou d'un certificat d'agrément ne respecte pas les obligations prescrites par les textes législatifs et réglementaires applicables, y compris celles de son cahier de charges, sur proposition de l'Autorité de régulation, le Ministre ayant le numérique dans ses attributions le met en demeure de s'y conformer dans un délai de quinze jours.

Lorsque le fournisseur de services numériques titulaire d'une autorisation ou d'un certificat d'agrément ne se conforme pas à la mise en demeure qui lui est adressée, le Ministre ayant le numérique dans ses attributions, par une décision motivée selon la gravité du manquement peut procéder à :

1) la réduction de la durée de validité du titre ;
2) la suspension du titre ;
3) le retrait du titre.

Les décisions de réduction de la durée de validité des titres, de suspension ou de radiation sont susceptibles de recours devant le Conseil d'Etat.

CHAPITRE II : DES DISPOSITIONS PÉNALES

Article 52.

Sous réserve des dispositions pénales en vigueur en République Démocratique du Congo, les infractions en matière du numérique peuvent donner lieu au paiement des amendes transactionnelles.

Les agents de l'Administration près le Ministère ayant le numérique dans ses attributions ainsi que ceux de l'Autorité de régulation ayant la qualité d'Officiers de police judiciaire, peuvent transiger avec le contrevenant et faire payer une amende transactionnelle dont les taux sont fixés par le Ministre ayant le numérique dans ses attributions.

Article 53.

Est puni d'une servitude pénale d'un à douze mois et d'une amende de quatre millions à vingt milliards de Francs congolais, tout fournisseur des services numériques soumis au régime d'autorisation ou de déclaration qui exerce en violation des dispositions des articles 33, 35 et 37 du présent Code.

Lorsque le fournisseur est une personne morale, la peine de servitude pénale s'applique à ses dirigeants.

CHAPITRE III : DE LA PRESCRIPTION

Article 54.

La prescription est acquise :

1) au profit des fournisseurs des services numériques dans leurs relations contractuelles avec les utilisateurs, pour toutes demandes en restitution du prix de leurs prestations présentées par un utilisateur après un délai d'un an à compter du jour du paiement ;
2) au profit des utilisateurs dans leurs relations contractuelles avec les fournisseurs des services numériques, pour les sommes dues à un fournisseur des services numériques au titre du paiement de ses prestations, lorsque celui-ci ne les a pas réclamées dans un délai d'un an à compter de la date de leur exigibilité.

LIVRE II : DES ÉCRITS ET OUTILS ELECTRONIQUES

TITRE I : DES DISPOSITIONS GÉNÉRALES

CHAPITRE I : OBJET ET CHAMP D'APPLICATION

Article 55.

Sans préjudice des dispositions légales particulières, le présent Livre traite des écrits et outils électroniques en République Démocratique du Congo.

Il s'applique également à toute suite de lettres, de caractères, de nombres, de chiffres, de symboles et tout autre signe sauvegardés qui a une signification compréhensible sur un support électronique, quelles que soient les modalités de leurs transmissions.

Article 56.

Il fixe les règles et principes applicables notamment à :

1) l'écrit électronique ;
2) la signature électronique ;
3) au cachet électronique ;
4) l'archivage électronique ;
5) l'horodatage électronique ;
6) la certification électronique ;
7) l'authentification des sites Internet.

TITRE II : DE L'ECRIT ELECTRONIQUE

CHAPITRE I : DES PRINCIPES GENERAUX

Article 57.

L'écrit électronique obéit aux principes de :

- intégrité ;
- liberté ;
- transparence ;
- clarté.

Article 58.

L'intégrité d'un écrit électronique résulte de :

1. la possibilité de vérifier que l'information n'en est pas altérée et qu'elle est maintenue dans son intégralité ;
2. la certitude que le support électronique portant l'information procure à celle-ci la stabilité et la pérennité voulues.

Article 59.

Nul ne peut être contraint de recourir à l'écrit électronique.

Article 60.

Toute personne qui recourt à l'écrit électronique s'assure que les informations, qu'elle appose sur un support électronique, garantissent un accès autorisé et utilisent un standard ouvert.

Article 61.

L'écrit électronique est constitué d'un contenu lisible et d'une qualité qui garantit sa compréhension.

CHAPITRE II : VALIDITÉ DE L'ÉCRIT ÉLECTRONIQUE

Article 62.

L'écrit électronique a la même valeur juridique que l'écrit sur support papier.

Article 63.

L'acte authentique peut être établi sur support électronique et a la même valeur juridique que l'acte authentique sur support papier.

Cet acte sur support électronique est soumise aux conditions de validité prévues dans la présent Code.

Un arrêté interministériel du Ministre ayant la Justice dans ses attributions et le Ministre du Numérique dans ses attributions, définit les conditions et modalités du présent article.

Article 64.

L'écrit électronique doit être horodatée et comporter une signature électronique certifiée.

L'horodatage et la signature électronique certifiée confèrent à l'écrit électronique la même valeur probante que l'écrit sur support papier légalisé ayant date certaine.

Article 65.

Sous réserve de dispositions légales particulières, lorsqu'un écrit est exigé pour la validité d'un acte juridique, il peut être établi et conservé sous forme électronique suivant les conditions prévues par le présent Livre.

Les documents ou titres que les textes légaux et réglementaires soumettent à des conditions particulières de forme et de fond, peuvent prendre la forme d'écrit électronique à condition qu'il respecte, en plus de ces exigences particulières, celles du présent Livre.

Article 66.

Peuvent notamment prendre la forme de l'écrit électronique suivant des règles particulières et spécifiques :

1) le contrat ;
2) les actes relatifs au droit civil des personnes ;
3) les actes relatifs aux sûretés personnelles ou réelles, de nature civile ou commerciale, sauf s'ils sont passés par une personne pour les besoins de sa profession ;
4) les actes qui créent ou qui transfèrent des droits réels sur des biens immobiliers ;
5) les actes juridiques pour lesquels la loi requiert l'intervention des Cours et Tribunaux ;
6) tous autres actes pour lesquels la loi exige non seulement un écrit sous format papier ou sous tout autre format autre que le format électronique, mais aussi certaines formalités particulières.

Les modalités d'équivalence ainsi que les spécificités techniques applicables aux matières prévues à l'alinéa précédent sont déterminées par arrêtés interministériels des Ministres sectoriels et celui ayant le numérique dans ses attributions.

CHAPITRE III : DE LA PREUVE ÉLECTRONIQUE

Article 67.

L'écrit électronique a la même valeur probante que l'écrit physique établi dans les mêmes conditions de validité.

Article 68.

La conservation des écrits sous forme des documents, enregistrements ou informations sous forme électronique satisfait aux exigences suivantes :

1. les documents, enregistrements, contenus ou informations électroniques conservés sont stockés de manière à être accessibles et consultables ultérieurement ;
2. les documents, enregistrements, contenus ou informations électroniques conservés demeurent au format auquel ils ont été générés, envoyés ou reçus, ou se trouvent dans

un format garantissant l'intégrité et l'exactitude des informations générées, envoyées ou reçues ;

3. les documents, enregistrements, contenus ou informations électroniques sont conservés sous un format permettant d'identifier, le cas échéant, leur origine et leur destination ainsi que les date et heure auxquelles ils ont été générés, envoyés et reçus pour la première fois, ainsi que celles auxquelles ils ont été conservés pour la première fois.

Les particularités techniques liées au format de conservation seront définies par l'Autorité de certification électronique.

Article 69.

Tout document, enregistrement, contenu ou toute information électronique satisfait aux obligations légales de présenter ou conserver les 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.

Article 70.

La copie ou la reproduction d'un acte sous forme électronique a la même valeur et force probante que l'acte lui-même à condition qu'elle conserve l'intégrité de l'acte électronique originaire.

L'intégrité peut être prouvée au moyen d'un certificat de conformité délivré par un prestataire de services de confiance conformément au Livre III du présent Code.

Article 71.

Dans les cas où il est exigé la production d'un document en format physique, une impression sur papier certifiée conforme à original peut être admise.

Cette certification est fournie par un prestataire de services de confiance conformément aux dispositions du Livre III du présent Code.

Article 72.

La remise d'un écrit sous forme électronique est effective lorsque le destinataire, après avoir pu en prendre connaissance, en a accusé réception.

Article 73.

Une communication électronique peut être faite par envoi recommandé avec accusé de réception. Dans ce cas, elle est acheminée par un tiers selon un procédé permettant de déterminer avec fiabilité et exactitude :

1. l'identité de l'expéditeur, du destinataire et du tiers qui achemine la communication électronique ;
2. la date et l'heure d'envoi du message ;
3. la date et l'heure de réception du message par le destinataire ;
4. le cas échéant, les données techniques relatives à l'acheminement du message de l'expéditeur au destinataire.
5. L'accusé de réception est adressé à l'expéditeur par voie électronique ou par tout autre moyen lui permettant de le conserver et de le reproduire.

Article 74.

Les données envoyées et reçues au moyen d'un service d'envoi électronique recommandé qualifié bénéficient d'une présomption quant à l'intégrité des données, de l'envoi de ces données par l'expéditeur identifié, à leur réception par le destinataire identifié et quant à l'exactitude de la date et de l'heure d'envoi et de réception indiquées par le service d'envoi recommandé électronique qualifié.

Article 75.

Les services d'envoi recommandé électronique qualifié doivent :

1. être fournis par un ou plusieurs prestataires de services de confiance qualifié ;
2. garantir l'identification de l'expéditeur avec un degré de confiance élevé ;
3. garantir l'identification du destinataire avec un degré de confiance élevé avant la fourniture des données ;
4. garantir que l'envoi et la réception des données sont sécurisés par une signature électronique certifiée ou par un cachet électronique qualifié d'un prestataire de services de confiance qualifié, de manière à exclure toute possibilité de modification des données;
5. garantir que toute modification des données nécessaire à l'envoi ou à la réception de celles-ci soit clairement identifiable et signalée à l'expéditeur et au destinataire des données. La date et l'heure d'envoi et de réception, ainsi que toute modification des données sont indiquées par un horodatage électronique qualifié.

Dans le cas où les données sont transférées entre deux prestataires de services de confiance qualifiés ou plus, les exigences prévues au présent article s'appliquent à tous les prestataires de services de confiance qualifiés.

TITRE III : DES OUTILS ELECTRONIQUES

CHAPITRE I : DE LA SIGNATURE ÉLECTRONIQUE

Article 76.

Sans préjudice des dispositions de la loi n° 18/019 du 09 juillet 2018 relative aux systèmes de paiement et de règlement-titres, la signature électronique est un élément de validité d'un acte juridique. Elle identifie celui qui l'appose et manifeste son consentement aux obligations qui en découlent.

Elle est admise dans les transactions électroniques à caractère commercial ou civil.

Article 77.

La fiabilité d'un procédé de signature électronique est présumée jusqu'à preuve du contraire, lorsque ce procédé met en œuvre une signature électronique qualifiée, établie grâce à un dispositif sécurisé de création de signature électronique et que la vérification de cette signature repose sur l'utilisation d'un dispositif qualifié.

Article 78.

La signature électronique qualifiée liée à un certificat électronique qualifié a la même force probante que la signature manuscrite.

Article 79.

Sauf preuve contraire, un document écrit sous forme électronique est présumé avoir été signé par son auteur et son texte est présumé ne pas avoir été modifié si une signature électronique qualifiée y est apposée.

La signature électronique qualifiée est celle qui résulte d'un procédé fiable d'identification qui garantit son lien avec l'acte auquel elle se rattache de telle sorte que toute modification ultérieure dudit acte est détectable.

Article 80.

La signature électronique qualifiée satisfait aux exigences suivantes :

1. être liée au signataire de manière univoque ;
2. permettre d'identifier le signataire ;
3. être créée à l'aide de données de création de signature électronique que le signataire peut, avec un niveau de confiance élevé, 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.

Article 81.

Les certificats qualifiés de signature électronique satisfont aux exigences d'intégrité prévues dans le présent Livre.

Les certificats qualifiés de signature électronique doivent garantir l'interopérabilité et la reconnaissance des signatures électroniques qualifiées au delà des frontières.

Article 82.

Un certificat qualifié de signature électronique révoqué après sa première activation perd sa validité à compter du moment de sa révocation.

Cette révocation n'emporte pas la validité antérieure du certificat, sauf s'il est établi que :

1. le certificat a été délivré sur base de fausses informations ;
2. le certificat a été délivré sur base d'une cause ou d'un objet illicite ;
3. le certificat a été délivré en violation des dispositions du présent Code.

Article 83.

Les dispositifs de création de signature électronique qualifiés respectent les exigences suivantes :

1. la garantie des moyens techniques et des procédures appropriées, notamment :
   - la confidentialité des données utilisées pour la création ;
   - la certitude que les données de vérification correspondent à celles de création ;
   - la fiabilité de la signature et la protection des données de sa création contre toute falsification par les moyens techniques ;
   - la fiabilité de la signature et la protection de ses données de création contre l'utilisation éventuelle par des tiers.
2. les dispositifs de création de signature électronique qualifiés ne modifient pas les données à signer et n'empêchent pas la présentation de ces données au signataire avant la signature ;
3. la génération ou la gestion de données de création de signature électronique pour le compte du signataire est exclusivement confiée à un prestataire de services de confiance qualifié.

Article 84.

Sans préjudice des dispositions de l'article précédent, un prestataire de services de confiance qualifié gérant des données de création de signature électronique pour le compte d'un signataire

ne peut reproduire les données de création de signature électronique qu'à des fins de sauvegarde, sous réserve du respect que :

1. le niveau de sécurité des ensembles de données reproduits doit être équivalent à celui des ensembles de données d'origine ;
2. le nombre d'ensembles de données reproduits n'excède pas le minimum nécessaire pour assurer la continuité du service.

Article 85.

La certification du dispositif de création de signature électronique qualifiée est assurée par l'Autorité de certification électronique suivant les exigences techniques fondamentales suivantes :

1. le système ou le produit dans lequel est mis en œuvre la clé privée de signature est certifié;
2. les systèmes ou les produits concourant à protéger cette clé privée contre une utilisation par d'autres que le signataire légitime, sont certifiés ;
3. la cryptographie repose sur une analyse théorique des mécanismes cryptographiques et sur une expertise de leur implémentation.

Un arrêté du Ministre ayant le numérique dans ses attributions détermine les exigences techniques supplémentaires éventuelles adaptées à l'évolution technologique ainsi que d'autres modalités opérationnelles nécessaires.

Article 86.

Le processus de validation d'une signature électronique qualifiée confirme sa validité aux conditions ci-après :

1. La conformité du certificat, sur lequel repose la signature au moment de la signature, aux exigences du présent Livre ;
2. la délivrance par un prestataire de services de confiance qualifié dudit certificat ainsi que sa validité au moment de sa signature ;
3. la correspondance des données de validation de la signature à celles communiquées à la personne concernée ;
4. la représentation unique et correcte des données fournies à la personne concernée ;
5. l'indication claire d'un pseudonyme s'il échet ;
6. la certitude qu'elle est créée par un dispositif de création qualifié et certifiée.

Article 87.

Les services de validation qualifié des signatures électroniques qualifiées ne peuvent être fournis que par un prestataire de services de confiance qualifié qui :

1. fournit une validation conformément aux exigences 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 qualifiée ou le cachet électronique qualifié du prestataire qui fournit le service de validation qualifié.

Article 88.

Un service de conservation qualifié des signatures électroniques qualifiées 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 II : DU CACHET ÉLECTRONIQUE

Article 89.

Le cachet électronique est admis dans les échanges et transactions électroniques, et renforce la validité de l'écrit électronique. Sa validité est soumise aux mêmes exigences que celles auxquelles est soumise la signature électronique conformément au présent Livre.

Un cachet électronique qualifié bénéficie d'une présomption d'intégrité des données et d'exactitude de l'origine des données auxquelles il est lié.

Article 90.

Un cachet électronique qualifié 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.

Article 91.

Sans préjudice des dispositions des articles 38 et 44 du présent Code, la fourniture du cachet électronique à un service répond aux exigences suivantes :

1) être un cachet électronique qualifié ;
2) être un cachet électronique qualifié reposant sur un certificat qualifié ;
3) être un cachet électronique qualifié au moins dans les formats ou utilisant les méthodes prévues arrêté visé à l'article 98 du présent Code.

Article 92.

Les cachets électroniques qualifiés exigés pour l'utilisation d'un service public en ligne sont :

1. les cachets électroniques qualifiés qui reposent sur un certificat qualifié ;
2. les cachets électroniques qualifiés au moins dans les formats ou utilisant les méthodes prévues par l'arrêté du Ministre visé à l'alinéa suivant du présent article.

Un arrêté du Ministre ayant le numérique dans ses attributions détermine les formats de référence des cachets électroniques qualifiés ainsi que les exigences supplémentaires d'usage des signatures et cachet électroniques dans le secteur public.

Article 93.

Les certificats qualifiés de cachet électronique répondent 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 de cachet électronique ;
2. un ensemble de données représentant sans ambiguïté le prestataire de services de confiance qualifié délivrant les certificats qualifiés, comprenant au moins :
   - pour une personne morale : le siège social, la dénomination et, le cas échéant, les informations d'identifications liées à son statut juridique ;
   - pour une personne physique : les prénom, nom et postnom de la personne.
3. le nom du créateur du cachet et, le cas échéant, les informations d'identifications liées à son statut juridique ;
4. la correspondance des données de validation du cachet électronique à celles de création ;
5. la validité du certificat ;
6. le code d'identité unique pour le prestataire de services de confiance qualifié ;
7. la signature électronique qualifiée ou le cachet électronique qualifié du prestataire de services de confiance qualifié délivrant le certificat ;
8. le lieu de délivrance du certificat sur lequel repose la signature électronique qualifiée ou le cachet électronique qualifié ;
9. l'emplacement des services qui peuvent être utilisés pour connaître le statut de validité du certificat qualifié.

Article 94.

Un dispositif de création de cachet électronique qualifié est un outil de création de cachet électronique qui satisfait mutatis mutandis aux exigences applicables aux dispositifs de création de signatures électroniques qualifiées.

Article 95.

Les critères de validation et de conservation des cachets électroniques qualifiés répondent mutatis mutandis aux dispositions applicables à la signature électronique.

CHAPITRE III : DE L'IDENTIFICATION ÉLECTRONIQUE

Section 1 : Des dispositions générales

Article 96.

L'identification électronique est un processus qui consiste à l'utilisation des données et éléments constitutifs de l'identité d'une personne physique ou morale par une forme électronique qui représente sans équivoque la personne physique ou morale concernée.

Article 97.

L'Etat peut procéder, au moyen d'identification électronique, à l'identification générale de la population et délivrer une carte d'identité biométrique à identifiant unique aux nationaux.

Une carte de résident à identifiant unique est délivrée aux étrangers résidant en République Démocratique du Congo.

Une carte de réfugié à identifiant unique est délivrée aux personnes en situation de réfugié en République Démocratique du Congo.

Article 98.

Sur proposition des Ministres ayant l'intérieur et le numérique dans leurs attributions, un décret du Premier Ministre délibéré en Conseil des Ministres détermine les critères d'authentification électronique et les spécifications techniques des moyens d'identification électronique.

Un arrêté du Ministre ayant le numérique dans ses attributions détermine également les schémas d'identification électroniques et leurs niveaux de garantie certifiant l'identification.

Section 2 : Schéma électronique

Article 99.

Un schéma d'identification électronique est éligible si :

1. les moyens d'identification relevant du schéma d'identification électronique peuvent être utilisés pour accéder à tout service fourni par une entité ou une administration publique exigeant une identification électronique ;

2. le schéma d'identification électronique et les moyens d'identification électronique délivrés répondent aux exigences d'au moins un des niveaux de garantie ;
3. l'identifiant électronique est attribué à la personne concernée conformément aux spécifications techniques, aux normes et aux procédures pour les niveaux de garantie.

Article 100.

Un schéma d'identification électronique détermine les spécifications des niveaux de garantie faible, substantiel et/ou élevé des moyens d'identification électronique délivrés dans le cadre dudit schéma.

Ces niveaux de garantie doivent satisfaire aux critères suivants :

1. **le niveau de garantie faible** est celui fourni par un moyen d'identification électronique qui accorde un degré limité de fiabilité à l'identité revendiquée ou prétendue d'une personne concernée. Il est caractérisé sur la base de spécifications techniques, de normes et de procédures y afférentes, y compris les contrôles techniques dont l'objectif est de réduire le risque d'utilisation abusive ou d'altération de l'identité de la personne concernée ;
2. **le niveau de garantie substantiel** est celui fourni par un moyen d'identification électronique qui accorde un degré substantiel de fiabilité à l'identité revendiquée ou prétendue d'une personne concernée. Il est caractérisé sur la base de spécifications techniques, de normes et de procédures y afférentes, y compris les contrôles techniques, dont l'objectif est de réduire substantiellement le risque d'utilisation abusive ou d'altération de l'identité de la personne concernée ;
3. **le niveau de garantie élevé** est celui fourni par un moyen d'identification électronique qui accorde un niveau de fiabilité à l'identité revendiquée ou prétendue d'une personne plus élevé qu'un moyen d'identification électronique à niveau de garantie substantiel. Il est caractérisé sur la base de spécifications techniques, de normes et de procédures y afférentes, y compris les contrôles techniques, dont l'objectif est d'empêcher l'utilisation abusive ou l'altération de l'identité.

Article 101.

Un décret du Premier Ministre délibéré en Conseil des Ministres sur proposition du Ministre ayant le numérique dans ses attributions fixe les spécifications techniques, normes et procédures minimales sur la base desquelles les niveaux de garanties faible, substantiel et élevé sont assurés par les moyens d'identification électronique prévus à l'article précédent.

Ces spécifications techniques, normes et procédures minimales sont fixées par référence à la qualité et à la fiabilité des éléments suivants :

1. la procédure visant à vérifier et prouver l'identité des personnes physiques ou morales demandant la délivrance de moyens d'identification électronique ;
2. la procédure de délivrance des moyens d'identification électronique demandés ;
3. le mécanisme d'authentification par lequel la personne concernée utilise/confirme son identité ;
4. l'entité délivrant les moyens d'identification électronique ;
5. tout autre organisme associé à la demande de délivrance de moyens d'identification électronique ;
6. les spécifications techniques et de sécurité des moyens d'identification électronique délivrés.

Article 102.

En cas d'atteinte à la sécurité ou d'altération du schéma d'identification électronique affectant la fiabilité de l'authentification de ce schéma, l'Autorité de certification électronique suspend et le cas échéant, le Ministre de tutelle révoque sans délai cette authentification ou les éléments altérés.

Lorsqu'il a été remédié à l'atteinte à la sécurité ou à l'altération visée à l'alinéa premier, l'autorité compétente rétablit l'authentification.

Article 103.

L'institution offrant un moyen d'identification électronique est responsable des dommages causés intentionnellement ou par sa négligence à tout utilisateur du moyen d'identification électronique.

Article 104.

Les schémas d'identification électronique sont interopérables.

Un décret du Premier Ministre délibéré en Conseil des Ministres sur proposition du Ministre ayant dans ses attributions le numérique fixe le cadre d'interopérabilité.

Article 105.

Les mesures d'applications assurent que ce cadre d'interopérabilité :

1. est technologiquement neutre et n'opère pas de discrimination entre les solutions techniques particulières destinées à l'identification électronique ;
2. suit, dans toute la mesure du possible, les normes et recommandations internationales;
3. facilite la mise en œuvre des principes du respect de la vie privée dès la conception ;

4. garantit que les données à caractère personnel sont traitées conformément aux dispositions de la loi, notamment les dispositions du Livre V du présent Code.

Article 106.

La fixation du cadre d'interopérabilité doit répondre aux exigences :

1. d'une référence aux exigences techniques minimales liées aux niveaux de garantie prévus à l'article 105 ;
2. d'une table de correspondances entre les niveaux de garantie des schémas d'identification électronique notifiés et les niveaux de garantie prévus à l'article 105 ;
3. d'une référence aux exigences techniques minimales en matière d'interopérabilité ;
4. d'une référence, dans le schéma d'identification électronique, à un ensemble minimal de données permettant d'identifier de manière univoque une personne physique ou morale;
5. de règles de procédure encadrant l'interopérabilité ;
6. de dispositions encadrant le règlement des litiges;
7. de normes opérationnelles communes de sécurité.

SECTION III : OBLIGATIONS LIÉES AU MOYEN D'IDENTIFICATION ÉLECTRONIQUE

Article 107.

Le titulaire d'un moyen d'identification électronique est tenu de prendre toutes les mesures nécessaires pour le garder sous son contrôle exclusif afin de prévenir le vol, la perte ou la divulgation. Dans ce cas, le titulaire doit immédiatement révoquer le moyen d'identification électronique.

Lorsque le moyen d'identification électronique vient à échéance ou est révoqué, son titulaire ne peut plus l'utiliser intentionnellement.

TITRE IV : DE L'HORODATAGE ÉLECTRONIQUE, DE L'ARCHIVAGE ÉLECTRONIQUE ET DE L'AUTHENTIFICATION DE SITES INTERNET

CHAPITRE I : DE L'HORODATAGE ÉLECTRONIQUE

Article 108.

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.

Article 109.

Tout horodatage électronique qualifié satisfait 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 qualifiée ou cachetée au moyen d'un cachet électronique qualifié du prestataire de services de confiance qualifié.

CHAPITRE II : DE L'ARCHIVAGE ÉLECTRONIQUE

Section 1 : Dispositions générales

Article 110.

Sous réserve des dispositions légales particulières, 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 sont conservées.

L'archivage électronique garantit l'authenticité et l'intégrité des documents, données et informations conservés par ce moyen.

Article 111.

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 éventuelle 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.

Section 2 : Des Archives numériques publiques

Article 112.

L'Institut National des Archives du Congo, en sigle « INACO », assure l'encadrement et la régulation des conditions générales de gestion des archives électroniques ainsi que l'assistance et le conseil aux services publics dans la gestion et la conservation des archives électroniques.

Article 113.

En plus de la tutelle du Ministre ayant la culture et le patrimoine dans ses attributions pour des aspects relatifs à la conservation de la mémoire continue de la nation, l'INACO relève également de la tutelle du Ministre ayant le numérique dans ses attributions pour les aspects relatifs à l'archivage numérique aux fins de garantir la convergence technologique.

Aux fins du financement de l'archivage des archives numérique publiques par l'INACO, une redevance est instituée sur tous les actes et documents émis par les services et établissements publics et destinés à être sauvegarder ou archiver. La redevance pour archivage est une quotité appliquée sur le prix de l'obtention desdits actes ou documents.

Le taux, la liste des actes et documents, ainsi que les mécanismes de perception, de recouvrement et de rétrocession à l'INACO de la redevance évoquée à l'alinéa précédent sont fixés par un arrêté interministériel des Ministres ayant respectivement les finances, le numérique et la culture et patrimoine dans leurs attributions.

CHAPITRE III : DE L'AUTHENTIFICATION DE SITES INTERNET

Article 114.

Les certificats qualifiés d'authentification de sites internet contiennent obligatoirement :

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 site internet ;
2. un ensemble de données représentant sans ambiguïté le prestataire de services de confiance qualifié délivrant les certificats qualifiés, comprenant au moins :
    - pour une personne morale : Le siège social et les informations d'identification liées à son statut juridique,
    - pour une personne physique: les prénom, nom et postnom ;

3. pour la personne physique, au moins le nom de la personne à qui le certificat a été délivré, ou un pseudonyme. Si un pseudonyme est utilisé, cela est clairement indiqué ;

4. Pour la personne morale, la dénomination de la personne à laquelle le certificat est délivré ainsi que les informations d'identification liées à son statut juridique ;

5. les éléments de l'adresse de la personne physique ou morale à laquelle le certificat est délivré et les éléments tels qu'ils figurent dans les registres officiels ;

6. le(s) nom(s) de domaine(s) exploité(s) par la personne physique ou morale à laquelle le certificat est délivré ;

7. des précisions sur le début et la fin de la période de validité du certificat ;

8. le code d'identité du certificat, qui doit être unique pour le prestataire de services de confiance qualifié ;

9. la signature électronique qualifiée ou le cachet électronique qualifié du prestataire de services de confiance qualifié délivrant le certificat ;

10. l'endroit où peut être obtenu le certificat sur lequel reposent la signature électronique qualifiée ou le cachet électronique qualifié visés au point 8 ;

11. l'emplacement des services de statut de validité des certificats qui peuvent être utilisés pour connaître le statut de validité du certificat qualifié.

Article 115.

Le certificat qualifié d'authentification de site internet est délivré par un prestataire de services de confiance qualifié et satisfait aux exigences prévues dans le présent Livre.

LIVRE III : DES PRESTATAIRES DE SERVICES DE CONFIANCE

TITRE I : DES DISPOSITIONS GENERALES

CHAPITRE I : OBJET ET CHAMP D'APPLICATION

Article 116.

Le présent livre traite des activités de prestataires de services de confiance établis en République Démocratique du Congo.

Il s'applique aussi aux prestataires de services de confiance établis à l'étranger dont les services sont destinés à la République Démocratique du Congo.

Il instaure un cadre juridique en matière de services de confiance afin de faciliter l'émergence du marché du numérique et de sécuriser les échanges de données par voie électronique entre les citoyens, les entreprises et les autorités publiques.

Article 117.

Le présent livre fixe :

1. les règles applicables aux services de confiance ;
2. les moyens de sécurisation des documents électroniques ;
3. les services de certificats pour la signature ou le cachet électronique, l'horodatage électronique, l'envoi recommandé électronique et l'authentification de site Internet.

Article 118.

Sont considérées comme services de confiance, les prestataires pour :

1. la signature électronique ;
2. le cachet électronique ;
3. l'horodatage électronique ;
4. l'archivage électronique ;
5. la certification électronique ;
6. l'authentification des sites internet ;
7. l'envoi recommandé électronique ;
8. la cryptologie.

Article 119.

Cette liste n'étant pas exhaustive, le Ministre ayant le Numérique dans ses attributions dispose du pouvoir de la compléter, l'Autorité de certification électronique entendue par avis écrit.

TITRE II : PRINCIPES ET CATEGORIES DES PRESTATAIRES

CHAPITRE I : DES PRINCIPES

Article 120.

Les prestataires de services de confiance obéissent aux principes de :

1. non-discrimination ;
2. équivalence fonctionnelle ;
3. neutralité technologique ;
4. autonomie.

Article 121.

Le prestataire de service de confiance est tenu de garantir indépendamment de toute considération, notamment de couleur, de sexe, de langue, de religion, d'origine nationale, ethnique ou sociale, l'intégrité et la fiabilité de ou des services de confiance qu'il fournit.

Article 122.

Le prestataire de service de confiance qui fournit un ou plusieurs services est libre d'utiliser toute technologie, certifiée par l'Autorité de certification électronique, qui garantit l'inviolabilité des plusieurs services de confiance fournis.

Article 123.

Les services de confiance fournis par un prestataire de services de confiance installé à l'étranger a la même valeur et est assimilé au service de confiance fourni par un prestataire de services de confiance établi en République Démocratique du Congo si l'une des deux conditions suivantes est remplie :

1. le prestataire de services de confiance doit avoir une représentation sur le territoire de la République Démocratique du Congo ;
2. le prestataire de services de confiance remplit les conditions prévues dans le présent Livre, après vérification par l'Autorité de certification électronique ;
3. le service de confiance ou le prestataire de services de confiance est reconnu en application d'un traité ou accord international dûment ratifié par la République Démocratique du Congo.

CHAPITRE II : DES CATÉGORIES DE PRESTATAIRES DE SERVICES DE CONFIANCE

Article 124.

Le présent Livre consacre deux catégories de prestataires de services de confiance :

1. Les prestataires de services de confiance qualifiés ;
2. Les prestataires de service de confiance non-qualifiés.

TITRE III : DU REGIME JURIDIQUE

CHAPITRE I : DE L'AUTORISATION ET DE LA DECLARATION

Article 125.

Sans préjudice des compétences exclusives dévolues aux notaires, aux huissiers de justice, à l'Institut National des Archives du Congo, ainsi qu'à la défense nationale et à la sûreté de l'Etat, toute personne physique ou morale, quelle que soit sa nationalité, désirant exercer les activités de prestation de service de confiance sur le territoire de la République Démocratique du Congo doit choisir l'un des régimes ci-après :

1. autorisation ;
2. déclaration.

Article 126.

Sont soumis au régime d'autorisation, les prestataires de services de confiance qualifiés, tandis que le régime de déclaration est exigé aux prestataires de services de confiance non-qualifiés.

Article 127.

L'autorisation et la déclaration s'effectuent conformément aux dispositions du chapitre IV du Livre premier du présent Code.

Article 128.

Les modalités pratiques d'exercice des activités relatives à la cryptologie et à des algorithmes spécialisés de sécurisation des données se font conformément aux dispositions du présent Code.

Un arrêté du Ministre ayant le numérique dans ses attributions détermine les modalités pratiques ainsi que les conditions d'exercice des activités visées à l'alinéa précédent.

Article 129.

Les prestataires de services de confiance non-qualifiés qui souhaitent des services de confiance qualifiés soumettent à l'Autorité de certification électronique une demande accompagnée d'un rapport d'évaluation de conformité.

Article 130.

L'Autorité de certification électronique vérifie notamment que le prestataire de services de confiance et les services de confiance fournis sont conformes aux dispositions du présent Code.

L'Autorité de certification électronique statue dans un délai de soixante jours à dater de la demande.

En cas de satisfaction aux conditions requises, elle accorde le statut de « qualifié » au prestataire requérant.

En cas de refus, elle statue par une décision motivée qu'elle signifie au requérant.

Article 131.

L'admission des prestataires de services de confiance à l'un des régimes juridiques prévus par le présent Code tient compte de :

1. infrastructures, des mesures techniques de sécurité et d'organisation mises en place par le prestataire ;
2. la régularité et de l'étendue des audits, certifiés, effectués pour vérifier la conformité de ses services à ses déclarations et politiques ;
3. garanties pécuniaires de sa responsabilité civile ;
4. garanties d'impartialité, d'indépendance et de probité du prestataire ;
5. l'accréditation ou de l'évaluation de la qualité de ses procédés de sécurisation déjà attribuée au prestataire établi à l'étranger par un organisme indépendant.

TITRE IV : OBLIGATIONS ET RESPONSABILITÉS

CHAPITRE I : DES OBLIGATIONS ET RESPONSABILITÉ DES PRESTATAIRES DE SERVICE DE CONFIANCE

Section 1 : Des obligations

Article 132.

Tout prestataire de services de confiance qualifié établi en République démocratique du Congo est tenu de soumettre à l'Autorité de certification électronique, notamment, les informations suivantes :

1. Pour une personne physique :
   - ses prénom, nom et post-nom ;
   - son domicile, son adresse de courrier électronique ainsi que son numéro de téléphone ;
   - sa signature électronique certifiée ;
   - son cachet électronique certifié ;
   - toutes les mentions obligatoires inhérentes à son statut juridique.
2. Pour une personne morale :
   - la preuve de l'immatriculation au RCCM ;
   - sa dénomination;
   - son siège social, son adresse de courrier électronique ainsi que son numéro de téléphone ;
   - sa signature électronique certifiée ;
   - son cachet électronique certifié ;
   - toutes les mentions obligatoires inhérentes à son statut juridique.

Article 133.

Le prestataire de services de confiance qualifié est tenu de :

1. informer l'Autorité de certification électronique 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 qualifié en toute sécurité ;
3. assurer le fonctionnement d'un service d'annuaire rapide et sûr et d'un service de révocation sûr et immédiat ;

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 électroniques, garantir la confidentialité au cours du processus de génération de ces données ;
6. souscrire à une police d'assurance garantissant les dommages susceptibles d'être causés dans l'exercice de cette activité ;
7. employer un personnel disposant de l'expertise, de l'expérience et des qualifications nécessaires en matière de sécurité des réseaux et systèmes d'information ;
8. 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 et doit être aisément compréhensible. Des éléments pertinents de cette information doivent également, sur demande, être mis à la disposition de tiers qui se prévalent du certificat ;
9. utiliser des systèmes et équipements fiables, protégés contre les risques de modifications et assurant la sécurité technique des processus pris en charge ;
10. utiliser des systèmes fiables de stockage des données qui lui sont communiquées, sous une forme vérifiable de sorte que :
    - les données ne soient publiquement disponibles pour des traitements qu'après avoir obtenu le consentement de la personne concernée ;
    - seuls les responsables de traitement puissent introduire des données et modifier les données conservées ;
    - l'authenticité des données puisse être vérifiée.
11. prendre les mesures appropriées contre la falsification, le piratage et le vol de données ;
12. enregistrer, conserver et maintenir accessibles pour une durée d'utilité administrative fixée dans un calendrier de conservation des archives, 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 ;
13. disposer d'un plan actualisé d'arrêt d'activités afin d'assurer la continuité du service ;
14. assurer le traitement licite des données à caractère personnel conformément aux dispositions du présent Code ;
15. le cas échéant, établir et tenir à jour une base de données des certificats octroyés ;
16. s'assurer que les certificats ne sont disponibles au public que dans les cas où le titulaire du certificat a donné son consentement ;

17. souscrire à une police d'assurance responsabilité civile.

Article 134.

Le prestataire de service de confiance est tenu d'adresser une notification motivée au bénéficiaire de service de confiance avant toute révocation du certificat.

Lorsque la révocation est effective, il est tenu de publier cette révocation dans le journal technique de ses serveurs.

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, au moins par certificat, à tout moment et au-delà de la période de validité du certificat, sous une forme automatisée, fiable, gratuite et efficace.

Article 135.

Sans préjudice des dispositions du Livre V du présent Code, le prestataire de services de confiance qui délivre des certificats au public ne peut 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 leur 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 intéressée.

Les prestataires ne peuvent détenir, consulter, exploiter et divulguer ces données que dans la mesure strictement nécessaire à l'accomplissement de leurs services.

Lorsque le titulaire du certificat utilise un pseudonyme et que 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'autorité compétente toute donnée et/ou information relative à l'identité du titulaire en sa disposition.

Article 136.

Les prestataires de services de confiance qualifiés et non-qualifiés sont tenus de prendre 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, 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, d'informer les parties concernées des effets préjudiciables de tels incidents et d'assurer la continuité des services en cas de défaillances techniques dans leur chef ou de cessation d'activité.

Article 137.

Les prestataires de services de confiance qualifiés et non-qualifiés notifient à l'Autorité de certification électronique par tout moyen, et le cas échéant, aux autres organismes concernés, dans un délai de vingt-quatre 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 138.

Lorsque l'atteinte à la sécurité ou la perte d'intégrité visée est susceptible de porter préjudice à un utilisateur du service de confiance, le prestataire de services de confiance lui notifie aussi l'atteinte à la sécurité ou la perte d'intégrité dans un délai de vingt-quatre heures.

Lorsque l'atteinte à la sécurité ou la perte d'intégrité concerne un Etat étranger, l'Autorité de certification électronique qui en a reçu la notification en informe préalablement les autorités compétentes. L'Autorité de certification électronique en informe par ailleurs le public ou exige du prestataire de services de confiance qu'il informe le public, dès lors que l'Autorité de certification électronique constate qu'il est dans l'intérêt du public d'être alerté de l'atteinte à la sécurité ou de la perte d'intégrité.

Article 139.

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 éléments d'identification 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.

Les moyens de vérification sont, notamment :

1. la présence physique de la personne concernée ou du représentant autorisé de la personne morale ;
2. le certificat de signature électronique qualifié ou de cachet électronique qualifié ;
3. d'autres méthodes d'identification reconnues en République Démocratique du Congo qui fournissent une garantie équivalente en termes de fiabilité, à la présence physique de la personne concernée ou du représentant autorisé de la personne morale. La garantie équivalente est confirmée par l'Autorité de certification électronique.

Article 140.

A la demande du titulaire du certificat préalablement identifié, de ses ayants droit ou ses mandataires, le prestataire de services de confiance révoque immédiatement le certificat.

Article 141.

Le prestataire de services de confiance révoque également un certificat lorsque :

1. il existe des raisons sérieuses qui indiquent 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 ont été violée ou risque de l'être ;
2. le prestataire de services de confiance prend les mesures nécessaires afin de répondre à tout moment et sans délai à une demande de révocation.

Article 142.

Lorsque la décision de la révocation est prise, le prestataire de services de confiance notifie la révocation du certificat au titulaire dans un délai de trente jours avant l'expiration du certificat. La décision de révocation doit être motivée.

Le titulaire du certificat dispose d'un délai de trente jours pour introduire un recours devant l'autorité compétente. Ce délai prend cours le jour de sa notification de cette décision par le prestataire de services de confiance.

Section 2 : De la responsabilité

Article 143.

Le prestataire de service de confiance est responsable des actes dommageables causés par négligence ou par maladresse à toute personne physique ou morale.

Dans ce cas, il incombe à la personne physique ou morale qui invoque les dommages d'en apporter la preuve.

Toutefois, dans le cas où le prestataire de service de confiance a informé préalablement la personne physique ou morale des limites technologiques de ses services et que ces limites ont été signalées à l'Autorité de certification électronique, il ne peut être tenu responsable des dommages survenus par l'utilisation des services au-delà de ses limites.

CHAPITRE II : OBLIGATION ET RESPONSABILITÉS DU TITULAIRE DU CERTIFICAT

Section 1 : De l'obligation

Article 144.

Le titulaire d'un certificat électronique est tenu de prendre toutes les mesures nécessaires pour le garder sous son contrôle exclusif afin de prévenir le vol, la perte ou la divulgation.

En cas de cas de vol, de perte ou de divulgation, le titulaire doit immédiatement informer le prestataire de service de confiance pour que ce dernier le révoque.

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 aux informations contenues dans le certificat, le titulaire a le droit de le faire révoquer.

Lorsqu'un certificat est arrivé à échéance ou a été révoqué, le titulaire ne peut, après expiration du certificat ou après révocation, utiliser les données relatives à la signature pour signer ou faire certifier ces données par un autre prestataire de services de confiance.

Section 2 : De la responsabilité

Article 145.

Tout acte pris avec un certificat volé, perdu ou divulgué sans que le titulaire n'ait pris des mesures pour sa révocation dans un délai raisonnable est réputé valable et engage le titulaire.

Le titulaire de certificat est responsable de tous dommages causés au tiers par des actes pris dans le contexte de l'alinéa précédent.

TITRE V : DU CONTROLE DES PRESTATAIRES DE SERVICES DE CONFIANCE

CHAPITRE I : DU CONTRÔLE

Article 146.

Le contrôle des activités des prestataires de services de confiance est exercé dans les conditions prévues par les lois et règlements en vigueur.

Article 147.

Les prestataires de services de confiance qualifiés font l'objet, au moins tous les vingt-quatre 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 les prestataires de services de confiance qualifiés et les services de confiance qualifiés qu'ils fournissent, remplissent les exigences fixées par le présent Code.

Dans un délai de dix jours ouvrables suivant sa réception, les prestataires de services de confiance qualifiés transmettent le rapport d'évaluation de conformité à l'Autorité de certification électronique électronique.

Article 148.

Sans préjudice des dispositions de l'article précédent, l'Autorité de certification électronique 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 les prestataires et les services de confiance qualifiés qu'ils fournissent, remplissent les exigences fixées dans le présent Livre.

Les contrôles inopinés de conformité réalisés par l'Autorité de certification électronique ne peuvent être abusifs et doivent être justifiés au regard de la situation du prestataire de services de confiance et des éléments le concernant dont il dispose.

Article 149.

L'Autorité de certification électronique tient à jour et publie des listes de confiance comprenant les informations relatives aux prestataires de services de confiance qualifiés, ainsi que les informations relatives aux services de confiance qualifiés qu'ils fournissent.

L'Autorité de certification électronique établit, tient à jour et publie de façon sécurisée et sous une forme adaptée au traitement automatisé, les listes de confiance visées à l'alinéa 1 relatives aux signatures électroniques et aux cachets électroniques.

L'Autorité de certification électronique met à la disposition du public, par l'intermédiaire d'un canal sécurisé, les informations visées aux alinéas précédents sous une forme portant une signature électronique ou un cachet électronique adaptée au traitement automatisé.

TITRE VI : DE LA CESSATION DES ACTIVITES

Article 150.

Le prestataire de services de confiance cesse ses activités :

1. si ses moyens technologiques et matériels ne garantissent plus la sécurité des certificats délivrés ;
2. s'il n'a plus de couverture financière nécessaire lui permettant d'assurer ses activités ;

3. s'il décide volontaire de quitter le secteur ;
4. s'il est sujet d'une sanction administrative.

Article 151.

Le prestataire de services de confiance informe l'Autorité de certification électronique avant soixante jours, 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. Ce transfert d'activités est réalisé sous le contrôle de l'Autorité de certification électronique.

En l'absence de repreneur, le prestataire révoque, sous réserve d'un préavis de deux mois, les certificats octroyés à ses titulaires.

Article 152.

Le prestataire de services de confiance qui arrête ses activités pour des raisons indépendantes de sa volonté ou en cas de faillite, en informe immédiatement l'Autorité de certification électronique. Il procède, le cas échéant, à la révocation des certificats délivrés.

TITRE VII : DES SANCTIONS

CHAPITRE I : DES SANCTIONS ADMINISTRATIVES

Article 153.

Lorsque le prestataire de services de confiance ne se conforme pas aux exigences fixées par l'Autorité de certification électronique, cette dernière peut prononcer à son encontre, dans le respect du principe du contradictoire, les sanctions suivantes :

1. l'injonction de cesser pour une durée de trois à douze mois la prestation de services de confiance et/ou le paiement d'une somme allant de cinq cents milles à cinq millions de Francs congolais lorsque l'impact du manquement se limite au titulaire ;
2. l'obligation par le prestataire de services de confiance d'informer immédiatement les titulaires des certificats qualifiés qu'il a délivrés, de leur non-conformité aux dispositions du présent Code et le paiement d'une somme allant de dix millions à cinquante millions de Francs congolais lorsque l'impact du manquement touche à l'intégrité de données personnelles des titulaires ;
3. l'interdiction d'exercer en République Démocratique du Congo, lorsque le manquement touche à la défense nationale ou à la sureté de l'Etat.

Article 154.

Lorsque l'Autorité de certification électronique exige du prestataire de services de confiance qualifié qu'il corrige un manquement aux exigences prévues dans le présent Code et que le prestataire n'agit pas en conséquence après expiration d'un délai raisonnable fixé par l'Autorité de certification électronique, cette dernière a la possibilité, en tenant compte de l'ampleur, de la durée et des conséquences du manquement, de retirer le statut « *qualifié* » au prestataire ou au service de confiance concerné, et en informe l'autorité compétente aux fins de la mise à jour des listes de confiance visées à l'article 131.

L'Autorité de certification électronique informe par ailleurs le prestataire de services de confiance qualifié du retrait de son statut « qualifié » ou du retrait du statut « qualifié » du service de confiance concerné.

Le retrait du statut de qualifié à un prestataire de services de confiance emporte sur les services qu'il fournit.

Un droit de recours est reconnu au prestataire de services de confiance dont la qualité de « qualifié » aura été retirée et s'exerce conformément à la loi.

CHAPITRE II : DES SANCTIONS PÉNALES

Article 155.

Est puni d'une peine de servitude pénale de six mois à cinq ans et d'une amende de cinq millions à cent millions de francs Congolais, ou d'une de ces peines seulement, quiconque aura usurpé la qualité de prestataire de services de confiance.

Les peines prévues à l'alinéa 1 sont portées au double en cas d'usurpation de la qualité de prestataire de services de confiance qualifié.

Article 156.

En condamnant du chef d'infraction visé à l'article 137, 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.

LIVRE IV : DU COMMERCE ET DES ECHANGES ELECTRONIQUES

TITRE I : DES DISPOSITIONS GENERALES

CHAPITRE I : OBJET ET CHAMP D'APPLICATION

Article 157.

Sans préjudice des dispositions légales et réglementaires applicables en matière commerciale ainsi que des principes généraux régissant les activités économiques et sociales, le commerce électronique est régi par les dispositions du présent Code.

Article 158.

Le présent Livre s'applique à tous les services commerciaux et des échanges par voie électronique de quelque nature que ce soit, prenant la forme des messages ou des documents électroniques.

Il s'applique aussi aux prestations des activités et services d'assurance, aux prestataires offrant des services de paiement mobile et électronique, aux intermédiaires commerciaux et des places de marché numériques « marketplace ».

Sans préjudice des dispositions de la loi n°18/019 du 09 Juillet 2018 relative aux systèmes de paiement et de règlement-titres, il s'applique également aux établissements de crédit, aux institutions de micro finance ainsi qu'aux services financiers intervenant par voie électronique.

Article 159.

Sont exclus du champ d'application du présent Livre :

1. les matières fiscale, parafiscale et douanière ;
2. les activités de jeux d'argent sous forme de jeu de hasard, de paris et de loterie ;
3. les activités de représentation et d'assistance en justice ;
4. les activités exercées par les notaires et les huissiers de justice ;
5. les contrats conclus entre professionnels en matière d'assurance, de sûreté, immobilière et dans les autres domaines où la loi exige des formalités administratives particulières.

CHAPITRE II : DES PRINCIPES RÉGISSANT LE COMMERCE ET LES ÉCHANGES ÉLECTRONIQUES

Article 160.

Le commerce et les échanges électroniques sont soumis aux principes ci-après :

1. la liberté d'exercice du commerce électronique ;
2. la responsabilité ;
3. l'obligation d'information et de transparence.

Article 161.

Le commerce électronique s'exerce librement sur tout le territoire de la République Démocratique du Congo, sous réserve des lois et règlements en vigueur.

Les atteintes, notamment à l'ordre et à la sécurité publics, à la protection des mineurs, à la protection de la santé publique, aux bonnes mœurs, à la défense nationale ou à la protection des personnes, constatées dans l'exercice ou à l'occasion de l'exercice du commerce électronique donnent lieu à des mesures de restriction et sont sanctionnées conformément à la présente loi ou aux dispositions légales et règlementaires en vigueur.

Un arrêté interministériel des Ministres ayant le commerce et le numérique dans leurs attributions détermine les modalités d'application des restrictions évoquées à l'alinéa précédent.

Article 162.

Toute personne physique ou morale exerçant les activités de commerce et des échanges électroniques est responsable de plein droit à l'égard de son contractant de la bonne exécution des obligations résultant du contrat conclu à distance, que ces obligations soient exécutables par elle-même ou par d'autres prestataires des services, sans préjudice de son droit de recours contre ceux-ci.

Toutefois, la personne peut s'exonérer de cette responsabilité en apportant la preuve que l'inexécution ou la mauvaise exécution du contrat est imputable soit à l'acheteur, soit à un cas de force majeure, soit à un tiers étranger à la fourniture des prestations prévues au contrat.

Article 163.

Sans préjudices des autres obligations prévues par les textes législatifs et réglementaires en vigueur, toute personne qui réalise une activité commerciale en ligne ou un échange électronique est tenue d'assurer aux clients auxquels est destinée la fourniture des biens et la prestation des services un accès facile, direct, permanent, tout en utilisant un standard ouvert aux informations suivantes :

1) Prénom, nom et post-nom, s'il s'agit d'une personne physique ;
2) Dénomination sociale, s'il s'agit d'une personne morale ;
3) Adresse complète de la résidence ou du siège social, son adresse de courrier électronique ainsi que le numéro de téléphone ;
4) Si elle est assujettie aux formalités d'inscription au registre du commerce, le numéro de son inscription au RCCM, le numéro d'identification national, le numéro d'identifiant fiscal, le capital social et l'adresse de son siège social ;
5) Si son activité est soumise à un régime quelconque d'autorisation préalable, l'adresse et la fonction de l'autorité ayant délivré celle-ci ;
6) Si elle est membre d'une profession réglementée, la référence aux règles professionnelles applicables, le titre professionnel, l'état dans lequel ce titre a été octroyé ainsi que la dénomination de l'ordre ou de l'organisme professionnel auprès duquel elle est inscrite ;
7) Le code de conduite auquel elle est éventuellement soumise ainsi que les informations relatives à la façon dont ces codes et informations peuvent être consultés par voie électronique.

Toute personne intervenant dans le commerce électronique mentionne les prix de son offre de manière claire et signale si les taxes et frais de livraison, notamment, y sont inclus.

L'obligation définie à l'alinéa précédent s'applique sans préjudice des autres obligations d'informations en matière de prix. Elle ne fait pas obstacle aux conditions de tarification et d'imposition prévue par les dispositions légales et réglementaires en vigueur.

TITRE II : DE LA PUBLICITE PAR VOIE ELECTRONIQUE

CHAPITRE I : DES DISPOSITIONS GENERALES

Section 1 : Identification des publicités par voie électronique

Article 164.

Toute publicité, sous quelque forme que ce soit, accessible par un service de communications électroniques ouvert au public ou un service en ligne, doit pouvoir être clairement identifiée comme telle dès sa réception.

Elle rend 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.

A défaut, elle comporte la mention *« publicité »* de manière claire, lisible, apparente et non équivoque, le cas échéant, dans l'objet ou dans le corps du message qui la véhicule.

Article 165.

Les offres promotionnelles proposant des réductions de prix, offres conjointes, primes ou cadeaux de quelque nature qu'ils soient, dès lors qu'elles sont adressées ou accessibles par voie de communications électroniques ouverte au public ou via un service en ligne, doivent être identifiables comme telles, dès réception par l'utilisateur ou dès que ce dernier y a accès.

Les conditions pour en bénéficier doivent être aisément accessibles et présentées de manière claire, précise et non équivoque.

De même, les concours ou jeux promotionnels doivent être clairement identifiables comme tels, dès leur réception par l'utilisateur ou dès que ce dernier y a accès.

Les conditions de participation aux concours ou jeux promotionnels doivent être aisément accessibles et présentées de manière claire, précise et non équivoque. Le cas échéant, les offres, concours et jeux promotionnels doivent être identifiables dans l'objet ou dans le corps du message qui les véhicule.

CHAPITRE II : DES CONDITIONS DE LA PROSPECTION DIRECTE

Article 166.

Est interdite, 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.

Pour l'application du présent article, 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 article, on entend par consentement, toute manifestation de volonté libre, spécifique et informée par laquelle une personne accepte que des données à caractère personnel la concernant soient utilisées à des fins de prospection directe.

L'absence de réponse ne peut pas être considérée comme un consentement.

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.

Article 167.

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 III de la présente loi, 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, si les coordonnées électroniques utilisées à cette fin sont impersonnelles.

Article 168.

Toute personne peut notifier directement à un fournisseur de biens ou services en ligne, sans justification et sans frais, sa volonté de ne plus recevoir de prospections directes. Dans ce cas, le fournisseur est tenu de :

1. délivrer, sans délai, un accusé de réception par tout moyen, y compris par voie électronique, confirmant à cette personne l'enregistrement de sa demande ;
2. prendre, dans un délai raisonnable, les mesures nécessaires pour respecter la volonté de cette personne ;
3. tenir à jour la liste des personnes qui ont exprimé leur volonté de ne plus recevoir de prospections directes de sa part.

Article 169.

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 et sans dol.

Article 170.

Dans tous les cas, 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 auxquels 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.

L'Autorité de protection des données prévue au Livre V veille, pour ce qui concerne la prospection directe utilisant les coordonnées d'un utilisateur personne physique, au respect des dispositions du présent Titre en utilisant les compétences qui lui sont reconnues.

A cette fin, elle peut notamment recevoir, par tous moyens, les plaintes concernant les manquements aux dispositions du présent article.

TITRE III : DES MÉCANISMES DE SÉCURISATION DES DONNÉES ET DES INFORMATIONS SOUS FORME ÉLECTRONIQUE

CHAPITRE I : DE LA PREUVE ÉLECTRONIQUE

Article 171.

La preuve par écrit ou preuve littéraire est établie conformément aux dispositions du présent Code.

La preuve des obligations contractuelles sous forme électronique obéit aux termes et délais fixés par les dispositions du présent livre.

Article 172.

L'écrit sous forme électronique est admis comme preuve au même titre que l'original de l'écrit sur 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 conformément à la législation relative à la conservation des archives.

Article 173.

Le fournisseur de biens ou prestataire de services par voie électronique qui réclame l'exécution d'une obligation doit en prouver l'existence.

Article 174.

Lorsque la loi n'a pas fixé d'autres principes et à défaut de conventions valables entre les parties, le juge règle les conflits de preuve littérale en déterminant par tous les moyens le titre le plus vraisemblable quel qu'en soit le support.

Article 175.

La copie ou toute autre reproduction d'actes passés par voie électronique a la même force probante que l'acte lui-même lorsqu'elle est certifiée conforme par le prestataire de services compétent conformément aux dispositions de l'article 113 du présent Code.

La certification donne lieu, le cas échéant, à la délivrance d'un certificat qualifié.

CHAPITRE II : DE LA SIGNATURE ÉLECTRONIQUE

Article 176.

Nul ne peut être contraint à signer électroniquement.

Article 177.

Lorsque la signature électronique, entendue aux termes des dispositions de l'article 2 du présent Code, est constatée par le prestataire de service de confiance compétent dans un certificat électronique, elle est admise au même titre que la signature autographe.

Article 178.

Toute personne utilisant un dispositif de signature électronique doit :

1. prendre les précautions minimales fixées par les lois en vigueur pour éviter toute utilisation illégale des équipements personnels relatifs à sa signature ;
2. informer, le cas échéant, l'Autorité de certification électronique compétente en la matière de toute utilisation illégale de sa signature ;
3. veiller à la véracité de toutes les données qu'elle a déclarées à ladite autorité ;
4. s'assurer de la véracité de toutes les données qu'elle a déclarée à toutes les personnes à qui elle a demandé de se fier à sa signature.

Article 179.

En cas de violation des dispositions de l'article précédent, le titulaire de la signature est responsable du préjudice causé à autrui.

TITRE IV : DU COMMERCE ELECTRONIQUE

CHAPITRE I : DE LA CONCLUSION DU CONTRAT SOUS FORME ELECTRONIQUE

Section 1 : Principe et contenu de l'offre

Article 180.

Quiconque propose, à titre professionnel, par voie électronique, la fourniture de biens ou la prestation de services, met à la disposition de la clientèle les conditions contractuelles applicables de manière à permettre leur analyse, leur conservation et leur reproduction.

Sans préjudice des conditions de validité mentionnées dans l'offre, son auteur reste engagé par elle tant qu'elle est accessible par voie électronique de son fait.

L'offre énonce en outre, notamment :

1. les caractéristiques essentielles du bien ou du service ;
2. les différentes étapes à suivre pour conclure le contrat par voie électronique ;
3. les moyens techniques permettant à l'utilisateur, avant la conclusion du contrat, d'identifier les erreurs et de les corriger ;
4. la durée de l'offre du produit ou du service ;
5. le prix du bien ou du service offert ;
6. les modalités et délais de paiement ;
7. les modalités et délais de livraison du bien ou de la fourniture de services ;
8. la ou les langue(s) proposée(s) pour la conclusion du contrat ;
9. en cas d'archivage du contrat, les modalités de cet archivage par l'auteur de l'offre et les conditions d'accès au contrat archivé ;
10. les dispositions relatives à la protection des données à caractère personnel ;
11. les conséquences de l'absence de confirmation des informations communiquées par le client;
12. les conséquences d'une inexécution ou d'une mauvaise exécution des obligations du fournisseur ;
13. le numéro de téléphone, ainsi que l'adresse électronique du fournisseur en vue d'éventuelles réclamations ;
14. les modalités prévues par le fournisseur pour le traitement des réclamations ;
15. 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 ;
16. l'existence ou l'absence d'un droit de rétractation et ses conditions d'exercice ;
17. le cas échéant, les modalités de retour, d'échange et de remboursement des biens ;
18. le cas échéant, les informations relatives à l'assistance après-vente, le service après-vente et les conditions y afférentes ;

19. le cas échéant, les informations relatives à la nature et l'étendue des garanties commerciales ;
20. les informations relatives aux garanties légales de conformité, garanties légales des vices cachés et garanties légales d'éviction.

Article 181.

Lorsqu'il est en mesure de le faire, le fournisseur de biens ou services en ligne met en place :

1) un service permettant aux clients de dialoguer directement avec lui ;
2) les moyens de consulter par voie électronique les règles professionnelles et commerciales auxquelles l'auteur de l'offre est soumis.

Les informations contenues dans l'offre sont fournies avant que le client du service ou du bien passe commande.

La commande par voie électronique est faite de manière claire, compréhensible et non équivoque.

Section 2 : Conditions de validité d'un contrat conclu par voie électronique

Article 182.

Le contrat par voie électronique est valablement conclu si le client accepte l'offre, après avoir eu, au préalable, la possibilité de vérifier et de réagir aux détails de sa commande.

L'auteur de l'offre accuse réception par voie électronique de la commande lui adressée conformément aux conditions de l'offre.

Dans le cas d'un contrat conclu entre un professionnel et un non-professionnel, les dispositions prévues à l'article 161 sont d'application.

La commande, la confirmation de l'acceptation de l'offre et l'accusé de réception sont considérés comme reçus lorsque les parties y ont accès par voie électronique.

Section 3 : Dérogations aux dispositions relatives au contenu d'un contrat conclu par voie électronique

Article 183.

Le contrat conclu par voie électronique peut déroger aux dispositions des articles 161 et 162 du présent Code dans les conventions conclues entre professionnels.

Section 4 : Responsabilité contractuelle des parties

Article 184.

Dès la conclusion du contrat électronique, le fournisseur est tenu de transmettre au client une copie électronique dudit contrat.

Toute vente de produit ou prestation de service par voie électronique donne lieu à l'établissement, par le fournisseur, d'une facture remise au client.

La facture doit être établie conformément à la législation et à la règlementation en vigueur.

CHAPITRE II : DE L'EXECUTION DU CONTRAT ELECTRONIQUE

Section 1 : Du paiement du prix ainsi que la livraison du produit et de la prestation des services

Article 185.

Sauf dispositions contraires prévues dans le contrat électronique, le client est tenu de payer le prix convenu dès sa conclusion.

Article 186.

A la livraison effective du produit ou à la fourniture du service objet du contrat électronique, le fournisseur doit exiger du client d'en accuser réception ; et le client est tenu d'accuser réception.

Une copie de l'accusé de réception est obligatoirement remise au client.

Sous réserve des dispositions de l'alinéa précédent, lorsque le fournisseur livre un produit et/ ou un service commandé par le client, il exige le paiement de son prix et de ses frais de livraison.

En cas de non-respect par le fournisseur des délais de livraisons, ou lorsque les conditions de l'offre ne sont pas remplies, le client peut réexpédier le produit dans un délai n'excédant pas quatre jours ouvrables à compter de la date de la livraison effectuée du produit et ce, sans préjudice de son droit de réclamer la réparation du dommage causé.

Dans ce cas, le fournisseur doit restituer au client le montant payé et les dépenses afférentes au retour du produit dans un délai de quinze jours à compter de la date de réception du produit.

Article 187.

Le fournisseur doit reprendre sa marchandise en cas de livraison d'un article non conforme à la commande ou dans le cas d'un produit défectueux.

Le client doit réexpédier la marchandise dans son emballage d'origine dans un délai maximal de sept jours augmentés de délai de distance conformément à la législation en vigueur, à compter de la date de livraison effective en indiquant le motif de refus, les frais étant à la charge du fournisseur.

A défaut pour le client de réexpédier la marchandise dans le délai prévu à l'alinéa précèdent, la marchandise est réputée être acceptée.

Le fournisseur est tenu de faire soit :

1. une nouvelle livraison conforme à la commande ;
2. une réparation du produit défectueux ;
3. un échange de produit par un autre identique ;
4. une annulation de la commande et un remboursement des sommes versées et ce, sans préjudice de la possibilité de demande de réparation par le client, en cas de dommage subi.

Le remboursement doit intervenir dans un délai de quinze jours à compter de la date de réception du produit.

Section 2 : De l'obligation de conserver les registres des transactions

Article 188.

Tout fournisseur opérant sur le territoire national est tenu de conserver les registres des transactions commerciales réalisées ainsi que leurs dates, et de les transmettre par voie électronique sur les plateformes de l'Institut National de statistiques, de l'Autorité de régulation, ainsi que du guichet unique du commerce extérieur dans le cas où la transaction s'opère avec un client se retrouvant en dehors du territoire de la République Démocratique du Congo, ou lorsque la prestation ou le bien objet de la transaction provient de l'étranger.

CHAPITRE III : DU DROIT DE RETRACTATION

Article 189.

Les dispositions du présent chapitre relatives au droit de rétractation ne s'appliquent qu'aux contrats conclus entre professionnel et non-professionnel.

Ces dispositions s'appliquent sans préjudices d'éventuelles dispositions conventionnelles plus favorables pour le non-professionnel.

Section 1 : Délai de rétractation

Article 190.

Sous réserve d'accord exprès entre les parties, avant le jour de l'expédition prévu dans le contrat, le client dispose d'un délai de soixante-douze heures au plus pour exercer son droit de rétractation.

Ce droit s'exerce par le client, sans justifications et sans frais, autres que les éventuels coûts directs de renvoi du bien au professionnel, le cas échéant.

Si les informations prévues aux articles 161 et suivants du présent Livre sont communiquées au non-professionnel avant la conclusion du contrat, le délai d'exercice du droit de rétractation commence à courir :

1. à compter du délai indiqué à l'alinéa précédent, s'agissant des contrats portant sur la fourniture de biens;
2. quarante-huit heures au plus de la passation de la commande, s'agissant des contrats portant sur la fourniture de services.

Si le professionnel manque à son obligation d'information préalable prévue aux articles 161 et suivants du présent Livre, le délai de rétractation est porté à quinze jours :

Le client notifie au professionnel sa décision d'exercer son droit de rétractation, par courrier électronique, dans le délai de soixante-douze heures au plus prévus à l'alinéa 1, ci-dessus.

Section 2 : Droits et obligations du professionnel

Article 191.

En cas d'exercice du droit de rétractation, le professionnel est tenu de rembourser toute somme reçue du client en paiement de sa commande ou liée à celle-ci. Ce remboursement intervient dans un délai maximum de soixante-douze heures, à compter de la date de réception par la notification de la rétractation.

Si le remboursement ne s'opère pas dans le délai prévu à l'alinéa précédent, les sommes dues au client sont, de plein droit, majorées au taux d'intérêt légal, à compter du lendemain de l'expiration du délai.

Section 3 : Perte du droit de rétractation et résolution ou résiliation de contrat

Article 192.

Le client perd son droit de rétractation, lorsque :

1. soit le bien a été livré et réceptionné par le client;
2. soit le service a été fourni ;
3. soit le délai légal de rétractation est forclos.

En cas d'exercice du droit de rétractation après le commencement de la fourniture du service, le client 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.

Article 193.

Sous réserve d'accord exprès entre les parties, le fournisseur exécute la commande dans un délai maximum de trente jours ouvrables, à compter du lendemain de la conclusion du contrat.

En cas de manquement contractuel du fournisseur après une mise en demeure de deux jours ouvrables restés sans suite, le client obtient de plein droit la résiliation du contrat, par simple notification adressée au fournisseur par courrier avec accusé de réception.

Le délai de réponse à toutes les demandes et réclamations du client est de soixante-douze heures.

En cas de résiliation du contrat par le client, le fournisseur est tenu de lui rembourser les sommes dues au titre du contrat, le cas échéant, dans un délai de cinq jours ouvrables à compter du jour de la notification de la résiliation par le client.

TITRE V : DES ÉCHANGES D'INFORMATIONS DANS L'ADMINISTRATION

Article 194.

Tout échange d'informations, de documents et/ou d'actes administratifs peut faire l'objet d'une transmission par voie électronique.

Lorsqu'il est prévu une exigence de forme particulière dans le cadre d'une procédure spéciale, cette exigence peut être satisfaite par voie électronique.

A cette fin, chaque administration communique les coordonnées électroniques permettant d'entrée en contact avec elle.

Toute personne physique ou morale qui souhaite être contactée par courrier électronique par l'administration lui communique les coordonnées nécessaires. Elle consulte régulièrement sa messagerie électronique et signale à l'administration tout changement de coordonnées.

Article 195.

Toute communication effectuée par voie électronique dans le cadre d'une procédure administrative est réputée réceptionnée au moment où son destinataire a la possibilité d'en prendre connaissance.

Un Décret du Premier Ministre délibéré en Conseil des Ministres sur proposition des Ministres ayant respectivement la fonction publique et le numérique dans leurs attributions en fixe les modalités de mise en œuvre.

LIVRE V : DE LA PROTECTION DES DONNEES A CARACTERE PERSONNEL

TITRE I : DISPOSITIONS GÉNÉRALES

CHAPITRE I : OBJET ET CHAMP D'APPLICATION

Article 196.

Le présent Livre fixe les règles relatives à la protection des données à caractère personnel.

Article 197.

Sans que cette liste ne soit exhaustive, les catégories suivantes sont considérées comme données à caractère personnel :

1. des données d'identification personnelle : prénom, nom, post-nom, date et lieu de naissance, âge, état civil, numéro d'identification nationale, document officiel d'identité en cours de validité ou toute autre donnée biométrique notamment photographie, enregistrement sonore, image, empreintes digitales et iris.
2. des données de correspondance : coordonnées téléphoniques, adresses physique, postale et électronique ;
3. des données professionnelles : statut, emploi occupé, employeur, rémunération ;
4. des données de facturation et de paiement : montant et historique des factures, état de paiement, relances, soldes de paiement, date de prélèvement ;
5. des coordonnées bancaires : code banque, numéro de compte et de la carte bancaire, nom / adresse / coordonnées de la banque, références de transactions ;
6. des données sur des personnes morales de droit public ou privé faisant apparaître des données personnelles ;
7. des données sur la situation familiale ;
8. des données concernant des décisions de justice.

Article 198.

Sont soumis aux dispositions du présent livre :

1) toute collecte, tout traitement, toute transmission, tout stockage et toute utilisation des données à caractère personnel par une personne physique, l'Etat, les collectivités locales, les personnes morales de droit public ou de droit privé ;
2) tout traitement automatisé ou non de données contenues ou appelées à figurer dans un fichier ;
3) tout traitement de données mis en œuvre sur le territoire national ;

4) tout traitement de données concernant la sécurité publique, la défense, la recherche et la poursuite d'infractions pénales ou la sûreté de l'Etat, sous réserve des dérogations définies par des dispositions spécifiques fixées par d'autres textes de loi en vigueur.

Article 199.

Sont exclus du champ d'application du présent livre :

1) les traitements de données mis en œuvre par une personne physique dans le cadre exclusif de ses activités personnelles ou domestiques, à condition que les données ne soient pas destinées à une communication systématique à des tiers ou à la diffusion ;
2) les copies temporaires faites dans le cadre des activités techniques de transmission et de fourniture d'accès à un réseau numérique, en vue du stockage automatique, intermédiaire et transitoire des données et à seule fin de permettre à d'autres destinataires du service le meilleur accès possible aux informations transmises.

TITRE II : DE L'AUTORITÉ DE PROTECTION DES DONNEES A CARACTERE PERSONNEL

CHAPITRE I : DE SON INSTITUTION ET DE SON STATUT

Article 200.

Il est créé une autorité de protection des données à caractère personnel », dénommée « Autorité congolaise de protection des données » en sigle « ACPD », ci-après désignée « Autorité de protection des données », chargée de contrôler le respect des dispositions du présent Livre et celles relatives à la protection de la vie privée et toute action étrangère touchant les données ou le traitement de données à caractère personnel hébergées en République Démocratique du Congo.

Article 201.

L'Autorité de protection des données est une autorité administrative indépendante dotée de la personnalité juridique et jouissant d'une autonomie administrative et financière.

Sur proposition du Ministre ayant le Numérique dans ses attributions, un décret délibéré en Conseil des Ministres fixe l'organisation et le fonctionnement de l'Autorité de protection des données.

Ses membres sont nommés par Ordonnance du Président de la République sur proposition du Ministre du Numérique pour une durée de 3 ans renouvelable et sont soumis au contrôle parlementaire.

Article 202.

L'Autorité de protection des données a pour mission de veiller à ce que les traitements des données à caractère personnel soient mis en œuvre conformément aux dispositions du présent Livre.

À ce titre, l'Autorité de protection des données est chargée :

1. de répondre à toute demande d'avis ou recommandation portant sur un traitement de données à caractère personnel ;
2. d'émettre de sa propre initiative des avis motivés ou des recommandations sur toute question relative à l'application des principes fondamentaux de la protection de la vie privée dans le cadre du présent Livre, ainsi que des lois contenant des dispositions relatives à la protection de la vie privée à l'égard des traitements de données à caractère personnel ;
3. d'informer les personnes concernées et les responsables de traitements de leurs droits et obligations ;
4. d'autoriser ou refuser les traitements de fichiers dans un certain nombre de cas, notamment les fichiers sensibles ;
5. de recevoir les formalités préalables à la création de traitements des données à caractère personnel et le cas échéant autoriser ces traitements ;
6. de recevoir, par la voie postale ou par voie électronique, les réclamations, les pétitions et les plaintes relatives à la mise en œuvre des traitements des données à caractère personnel et informer leurs auteurs des suites données à celles-ci notamment si un complément d'enquête ou une coordination avec une autre Autorité de protection nationale est nécessaire ;
7. d'effectuer, sans préjudice de toute action devant les tribunaux, des enquêtes, soit de sa propre initiative, soit à la suite d'une réclamation ou à la demande d'une autre Autorité de protection nationale, et informe la personne concernée, si elle l'a saisie d'une réclamation, du résultat de ses enquêtes dans un délai raisonnable ;
8. d'informer sans délai l'autorité judiciaire pour certains types d'infractions dont elle a connaissance ;
9. d'informer, sans délai, le Procureur de la république, conformément aux dispositions du code pénal, des violations des dispositions du présent Livre, constitutives d'infractions pénales ;
10. d'informer l'Assemblée nationale, le Gouvernement ou d'autres institutions politiques, ainsi que le public, de toute question relative à la protection des données à caractère personnel ;
11. de conduire de fréquentes consultations avec des parties prenantes sur des questions que l'Autorité considère comme pouvant nuire à la protection effective des données à caractère personnel pour les services, les installations, les appareils ou les annuaires au titre du présent Livre ;

12. de requérir des experts ou agents assermentés, en vue de participer à la mise en œuvre des missions de vérification portant sur tout traitement des données à caractère personnel sur le territoire de la République Démocratique du Congo ;
13. de veiller au respect des autorisations et consultations préalables ;
14. de prononcer la rectification, l'effacement ou la destruction de toutes les données lorsqu'elles ont été traitées en violation des dispositions du présent Livre et la notification de ces mesures aux tiers auxquels les données ont été divulguées ;
15. de demander au responsable du traitement ou au sous-traitant de satisfaire aux demandes d'exercice des droits prévus par les dispositions du présent Livre présentées par la personne concernée ;
16. de prononcer des sanctions administratives et pécuniaires, à l'égard des responsables de traitement ;
17. de mettre à jour un répertoire des traitements des données à caractère personnel et à la disposition du public ;
18. de surveiller les faits nouveaux présentant un intérêt, dans la mesure où ils ont une incidence sur la protection des données à caractère personnel, notamment l'évolution des technologies de l'information et des communications et celle des pratiques commerciales ;
19. d'informer le responsable du traitement ou le sous-traitant d'une violation alléguée des dispositions régissant le traitement des données à caractère personnel et, le cas échéant, d'ordonner au responsable du traitement ou son sous-traitant de remédier à cette violation par des mesures déterminées, afin d'améliorer la protection de la personne concernée ;
20. de conseiller les personnes physiques ou morales qui procèdent à des traitements des données à caractère personnel ou à des essais ou expériences de nature à aboutir à de tels traitements ;
21. d'autoriser ou refuser des transferts transfrontaliers de données à caractère personnel vers des États tiers ;
22. de sensibiliser le public aux risques, aux règles, aux garanties et aux droits relatifs au traitement des données à caractère personnel. Les activités destinées spécifiquement aux enfants, personnes âgées ou personnes gravement malades ou à tous ceux qui ne peuvent pas être en mesure de comprendre la portée des activités qui leur sont proposées, font l'objet d'une attention particulière ;
23. de faire des propositions de modifications législatives ou réglementaires susceptibles de simplifier et d'améliorer le cadre législatif et réglementaire à l'égard du traitement des données ;
24. d'homologuer les codes de conduite et de recueillir et d'autoriser, le cas échéant, les projets, modifications ou prorogations desdits codes ;
25. de mettre en place des mécanismes de coopération avec les autorités de protection des données à caractère personnel d'États tiers dont le partage d'informations et l'assistance mutuelle ;

26. de participer aux négociations internationales en matière de protection des données à caractère personnel ;
27. d'assurer le renforcement de capacités des responsables de traitement ou leurs délégués, des sous-traitants et leurs préposés.

TITRE III : CONDITIONS, PRINCIPES DE TRAITEMENT, DE TRANSMISSION ET DE TRANSFERT DES DONNEES A CARACTERE PERSONNEL ET DES ACTIVITES DE REGISTRE PUBLIC

CHAPITRE I : CONDITIONS DE TRAITEMENT DES DONNEES A CARACTERE PERSONNEL

Article 203.

Le traitement des données à caractère personnel est soumis à une déclaration préalable auprès de l'Autorité de protection des données.

La déclaration est effectuée par le responsable de traitement ou son représentant.

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

L'Autorité de protection des données délivre un récépissé en réponse à la déclaration, le cas échéant par voie électronique. Le demandeur peut mettre en œuvre le traitement dès réception de son récépissé; il n'est exonéré d'aucune de ses responsabilités.

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

Les conditions et la procédure de la déclaration sont fixées par l'Autorité de protection des données.

Article 204.

Sont soumis à une autorisation préalable de l'Autorité de protection des données avant toute mise en œuvre :

1. le traitement des données à caractère personnel portant sur des données génétiques, médicales et sur la recherche scientifique dans ces domaines ;
2. le traitement des données à caractère personnel portant sur des données relatives aux infractions, aux condamnations ou aux mesures de sûreté prononcées par les juridictions ;

3. le traitement portant sur un numéro national d'identification ou tout autre identifiant de la même nature, notamment les numéros de téléphones ;
4. le traitement des données à caractère personnel comportant des données biométriques ;
5. le traitement des données à caractère personnel ayant un motif d'intérêt public notamment à des fins historiques, statistiques ou scientifiques ;
6. le transfert de données à caractère personnel envisagé à destination d'un pays tiers.

La demande d'autorisation est présentée par le responsable du traitement ou son représentant.

L'autorisation n'exonère pas de la responsabilité à l'égard des tiers.

Les conditions et la procédure d'autorisation sont fixées par l'Autorité de protection des données.

Article 205.

Les demandes de déclaration et d'autorisation doivent au moins contenir :

1) l'identité ou la dénomination sociale, l'adresse complète du responsable du traitement ou, si celui-ci n'est pas établi sur le territoire de la République Démocratique du Congo, les coordonnées de son représentant dûment mandaté ;
2) la ou les finalités du traitement ainsi que la description générale de ses fonctions ;
3) les interconnexions envisagées ou toutes autres formes de mise en relation avec d'autres traitements ;
4) les données à caractère personnel traitées, leur origine et les catégories de personnes concernées par le traitement ;
5) le ou les services chargés de mettre en œuvre le traitement ainsi que les catégories de personnes qui, en raison de leurs fonctions ou pour les besoins du service, ont directement accès aux données enregistrées ;
6) les destinataires ou catégories de destinataires habilités à recevoir communication des données;
7) la fonction de la personne ou le service auprès duquel s'exerce le droit d'accès ;
8) les dispositions prises pour assurer la sécurité des traitements et des données dont les garanties qui doivent entourer la communication aux tiers ;
9) l'indication du recours à un sous-traitant ;
10) les transferts de données à caractère personnel envisagés à destination d'un État tiers, sous réserve de réciprocité ;
11) l'engagement que les traitements sont conformes aux dispositions du présent Livre.

L'Autorité de protection des données peut définir d'autres informations devant être contenues dans les demandes de déclaration et d'autorisation.

Article 206.

Sont dispensés des formalités de déclaration préalable :

- le traitement de données utilisées par une personne physique dans le cadre exclusif de ses activités personnelles, domestiques ou familiales ;
- le traitement de données concernant une personne physique dont la publication est prescrit par une disposition légale ou règlementaire ;
- le traitement de données ayant pour seul objet la tenue d'un registre qui est destiné à un usage exclusivement privé ;
- le traitement pour lequel le responsable de traitement a désigné un délégué à la protection des données à caractère personnel chargé d'assurer, d'une manière indépendante, le respect des obligations prévues dans le présent Livre, sauf lorsqu'un transfert de données à caractère personnel à destination d'un pays tiers est envisagé.
- les traitements des données à caractère personnel mis en œuvre par les organismes publics ou privés pour la tenue de leur comptabilité générale ;
- le traitement des données à caractère personnel mis en œuvre par les organismes publics ou privés relatifs à la gestion des rémunérations de leurs personnels ;
- les traitements des données à caractère personnel mis en œuvre par les organismes publics ou privés pour la gestion de leurs fournisseurs ;
- 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 doivent pas être communiquées à des tiers.

Article 207.

L'Autorité de protection des données doit se prononcer dans un délai de trente jours à compter de la réception de la demande de déclaration ou d'autorisation.

Toutefois, ce délai peut être prorogé une fois, de quinze jours sur décision motivée de l'Autorité de protection des données.

Si la déclaration ou l'autorisation demandée à l'Autorité de protection des données n'est pas rendu dans le délai prévu, la réponse vaut rejet.

Toutefois, il est accordé au responsable du traitement le droit de recours dans un délai de quinze jours.

Article 208.

La demande de déclaration ou d'autorisation peut être adressée à l'Autorité de protection des données par voie électronique ou par voie postale ou par tout autre moyen contre remise d'un accusé de réception par ladite Autorité.

CHAPITRE II : DU TRAITEMENT DES DONNEES A CARACTERE PERSONNEL

Article 209.

Le traitement de données à caractère personnel doit se faire dans le cadre du respect de la dignité humaine, de la vie privée et des libertés publiques.

Le traitement des données à caractère personnel, quel que soit son origine ou sa forme, ne doit pas porter atteinte aux droits des personnes protégées par les lois et règlements en vigueur et il est, dans tous les cas, interdit d'utiliser ces données pour porter atteinte aux personnes ou leur réputation.

Article 210.

Les données à caractère personnel doivent être :

1. traitées de manière licite, loyale et transparente :
   - la personne concernée donne expressément son consentement préalable. Si la personne concernée est incapable, le consentement est régi selon le principe de droit commun ;
   - la collecte de données est faite pour des finalités déterminées, explicites et légitimes ;
   - les données collectées ne sont pas traitées ultérieurement de manière incompatible avec les finalités visées au point précédent, compte tenu de tous les facteurs pertinents, notamment des prévisions raisonnables de l'intéressé et des dispositions légales et réglementaires applicables.
   - le principe de transparence implique une information obligatoire et claire ainsi qu'intelligible de la part du responsable du traitement portant sur les données à caractère personnel.
2. traitées de manière confidentielle et protégée, notamment lorsque le traitement comporte des transmissions de données dans un réseau ;
3. conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées. Les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, pour autant que soient

mises en œuvre les mesures techniques et organisationnelles appropriées requises par les dispositions du présent Livre afin de garantir les droits et libertés de la personne concernée sous réserve des dispositions de la 78-013 du 11 juillet 1978 portant régime général des archives ;

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

Article 211.

Les données à caractère personnel collectées doivent être fiables, adéquates, pertinentes, exactes, intègres et non excessives.

Toutes les mesures raisonnables doivent être prises afin que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées.

Article 212.

Est interdit, le traitement des données à caractère personnel ayant trait aux informations raciales, ethniques, aux opinions politiques, aux convictions religieuses ou philosophiques, aux statuts des refugiés et des apatrides, à l'appartenance syndicale, à la vie sexuelle ou plus généralement celles relatives à l'état de santé de la personne concernée.

L'interdiction de traiter des données à caractère personnel visées à l'alinéa 1 du présent article ne s'applique pas dans les cas suivants :

1. le traitement des données à caractère personnel portant sur des données manifestement rendues publiques par la personne concernée ;
2. la personne concernée a donné son consentement explicite au traitement de ces données à caractère personnel pour une ou plusieurs finalités spécifiques, sauf lorsque la législation en vigueur en République Démocratique du Congo prévoit que l'interdiction visée à l'alinéa 1 ne peut pas être levée par la personne concernée. Le consentement peut être retiré à tout moment sans frais par la personne concernée ;
3. le traitement des données à caractère personnel est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement ;
4. le traitement des données à caractère personnel s'avère nécessaire pour un motif d'intérêt public ;

5. le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou est effectué par une autorité publique ou est assigné par une autorité publique au responsable du traitement ou à un tiers, auquel les données sont communiquées ;
6. le traitement est effectué en exécution de lois relatives aux statistiques publiques ;
7. le traitement est nécessaire aux fins de médecine préventive ou la médecine du travail, de diagnostics médicaux, 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 agissant dans l'intérêt de la personne concernée et le traitement est effectué sous la surveillance d'un professionnel de santé ;
8. le traitement est nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique, tel que la protection contre les menaces transfrontalières graves pesant sur la santé, aux fins de garantir des normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux sur la base du droit en vigueur, qui prévoit des mesures appropriées et spécifiques pour la sauvegarde des droits et libertés de la personne concernée, notamment le secret professionnel ;
9. le traitement est nécessaire à la réalisation d'une finalité fixée par ou en vertu des dispositions du présent Livre, en vue de l'application de la sécurité sociale ;
10. 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 pendant la période précontractuelle;
11. le traitement est nécessaire au respect d'une obligation légale ou réglementaire à laquelle le responsable du traitement est soumis ;
12. le traitement est nécessaire afin d'exécuter les obligations et les droits spécifiques du responsable du traitement en matière de droit du travail ;
13. le traitement est effectué par des associations dotées de la personnalité juridique ou par des établissements d'utilité publique qui ont pour objet social principal la défense et la promotion des droits de l'homme et des libertés fondamentales, en vue de la réalisation de cet objet, à condition que ce traitement soit autorisé par l'Autorité de protection des données et que les données ne soient pas communiquées à des tiers sans le consentement écrit des personnes concernées, que ce soit sur un support papier, support électronique ou tout autre support équivalent ;
14. le traitement est effectué dans le cadre des activités légitimes et moyennant les garanties appropriées d'une fondation, d'une association ou de tout autre organisme à but non lucratif et à finalité politique, philosophique, religieuse, mutualiste ou syndicale. Toutefois, le traitement doit se rapporter exclusivement aux membres ou anciens membres de cet organisme ou aux personnes entretenant avec lui des contacts réguliers liés à ses objectifs et à sa finalité, et que les données ne soient pas communiquées à un tiers extérieur sans le consentement des personnes concernées ;

15. le traitement est nécessaire à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques.

Les données à caractère personnel visées à l'alinéa 1 peuvent faire l'objet d'un traitement aux fins prévues à l'alinéa 2, point 8, si ces données sont traitées par un professionnel de santé soumis à une obligation de secret professionnel conformément au droit en République Démocratique du Congo ou aux règles arrêtées par les organismes nationaux compétents, ou sous sa responsabilité, ou par une autre personne également soumise à une obligation de secret conformément au droit en République Démocratique du Congo ou aux règles arrêtées par les organismes nationaux compétents.

Article 213.

Dans les cas où le traitement repose sur le consentement, le responsable du traitement est 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, le formulaire sur la demande de consentement est rempli sous une forme qui le distingue clairement de ces autres questions, de façon 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 contraignante.

La personne concernée a le droit de retirer son consentement à tout moment, à travers le même moyen utilisé pour le donner. Le retrait du consentement ne compromet pas la licéité du traitement fondé sur le consentement effectué avant ce retrait. La personne concernée en est informée avant de donner son consentement. Il doit être 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 au traitement de données à caractère personnel qui n'est pas nécessaire à l'exécution dudit contrat.

CHAPITRE III : DE LA TRANSMISSION ET DU TRANSFERT DES DONNEES A CARACTERE PERSONNEL

Section 1. De la transmission des données à caractère personnel

Article 214.

La transmission de données à caractère personnel est licite et légale.

Elle se fait entre responsable de traitement de droit privé et/ou de droit public.

Article 215.

Un responsable de traitement peut transmettre à un ou plusieurs autres responsables de traitement des données à caractère personnel pour besoin de prospection ou tout autre besoin licite et légal avec le consentement de la personne concernée.

Le responsable de traitement qui transmet, veille à ce que les données communiquées ne soient altérées par quoi que ce soit.

Il s'assure de l'identité et de la qualité du responsable du traitement ou de son représentant qui reçoit les données.

Le responsable de traitement qui reçoit les données est tenu de les utiliser que pour de raisons pour lesquelles elles lui ont été communiquées.

L'accord de confidentialité est conclu entre les deux responsables de traitement.

Article 216.

Sur demande de l'Autorité de protection des données, tout responsable de traitement est tenu de communiquer des données à caractère personnel dont il a la gestion. De même, pour de raisons d'enquête judiciaire, le Ministère public peut adresser une réquisition d'information ou une requête au responsable de traitement.

Après s'être assuré de l'authenticité et de la régularité de la demande ou de la réquisition, le responsable de traitement y donne une réponse dans un délai qui ne peut dépasser deux jours.

Toutefois, dans le cas où il se trouve dans l'incapacité de répondre à la demande ou à la réquisition de l'autorité, le responsable de traitement en informe l'auteur de la demande ou de la réquisition au lendemain du délai fixé à l'alinéa 2 et prend toutes les dispositions pour y répondre dans un délai qui ne peut dépasser 8 jours.

Pour de raisons de sécurité nationale, l'Autorité de protection des données formule une correspondance au responsable de traitement pour que lui soient transmises toutes les informations nécessaires.

Article 217.

Lors de la communication des données à caractère personnel, cette opération doit comporter notamment l'identité du responsable qui a transmis les données au partenaire et ou sous-traitant, les droits de la personne concernée et notamment son droit de s'opposer à de la prospection.

Section 2 : Du transfert des données à caractère personnel

Article 218.

Les données à caractère personnel sont stockées et ou logées en République Démocratique du Congo.

Toutefois, pour des besoins de souveraineté numérique et de sécurité, les données à caractère personnel peuvent être transférées vers une ambassade digitale, un hébergeur se trouvant dans un État tiers ou une organisation internationale lorsque l'Autorité de protection de données constate que l'État ou l'Organisation Internationale en question assure un niveau de protection équivalent à celui mis en place par les dispositions du présent Livre.

Le caractère équivalent et suffisant du niveau de protection s'apprécie au regard de toutes les circonstances relatives à un transfert de données.

Afin de déterminer ce caractère équivalent et suffisant, il est notamment tenu compte de:

1) l'état de droit, le respect des droits de l'homme et des libertés fondamentales, la législation pertinente, tant générale que sectorielle ainsi que les droits effectifs et opposables dont bénéficient les personnes concernées et les recours administratifs et judiciaires que peuvent effectivement introduire les personnes concernées dont les données à caractère personnel sont transférées ;
2) l'existence et le 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 et de les faire appliquer, y compris par des pouvoirs appropriés d'application desdites règles, d'assister et de conseiller les personnes concernées dans l'exercice de leurs droits;
3) les 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 ce qui concerne la protection des données à caractère personnel.

Avant tout transfert effectif de données à caractère personnel vers un État tiers ou une organisation internationale, le responsable du traitement doit préalablement obtenir l'autorisation de l'Autorité de protection des données à caractère personnel.

Le transfert de données à caractère personnel vers des États tiers ou une organisation internationale fait l'objet d'un contrôle régulier de l'Autorité de protection des données à caractère personnel.

Article 219.

Le transfert de données à caractère personnel vers un État tiers ou une organisation internationale et n'assurant pas un niveau de protection adéquat, peut être effectué dans un des 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 du traitement ou des mesures préalables à la conclusion de ce contrat, prises à la demande de la personne concernée ;
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 du traitement et un tiers ;
4) le transfert est nécessaire ou rendu juridiquement obligatoire pour la sauvegarde d'un intérêt public important, ou pour la constatation, l'exercice ou la défense d'un droit en justice ;
5) le transfert est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée;
6) le transfert intervient au départ 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 du public 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.

Sans préjudice des dispositions de cet article, le Conseil des Ministres peut, et après avis conforme de l'Autorité, autoriser un transfert ou un ensemble de transferts de données à caractère personnel vers un État tiers ou une organisation internationale n'assurant pas un niveau de protection adéquat et suffisant, lorsque le responsable du traitement offre des garanties suffisantes au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes, ainsi qu'à l'égard de l'exercice des droits correspondants.

CHAPITRE IV : DES ACTIVITES DES REGISTRES PUBLICS

Article 220.

Les registres publics de données sont des bases de données contenant diverses informations récoltées par des systèmes sectoriels. Étant de plus en plus souvent informatisés et capables

d'échanger des données, les registres constituent une ressource inestimable de mise en place de la gouvernance numérique.

Les registres publics de données sont classés en plusieurs catégories notamment :

1. Registre National de la Population : registre de l'identité, registre de l'état civil, registre biométrique ;
2. Registres des terrains et propriétés : registre cadastral, registre de propriété, registre des actes notariés immobiliers, registre des baux, registre des mines, registre forestier, registre agricole ;
3. Registres de permis et licences : registre de concessions, registre des licences commerciales et / ou permis, registre personnel des licences et / ou permis, registre de permis de conduire ;
4. Registres des entreprises et de l'emploi : registre des entreprises, registre des contrats de travail et registre de l'industrie ;
5. Registres des factures et paiements : registre des factures, registre des points de vente, registre du commerce électronique et registre des paiements électroniques ;
6. Registre des citoyens et des migrants : registre des personnes physiques, registre des bénéficiaires effectifs et registre des visas ;
7. Registre des actifs : registre des véhicules automobiles, registre téléphonique, registre des aéroports;
8. Registre de la santé, de l'éducation, des activités sociales, etc.

Des données extraites de ces registres sont utilisées dans de nombreux services administratifs, que ce soit sous la forme de certificats ou via un accès direct à ces données lorsqu'elles sont numériques.

Le Ministre ayant le numérique dans ses attributions, en collaboration avec les Ministres sectoriels, élabore les cahiers de charge technique de la conception et de la mise en œuvre de registres publics de données après avis de l'Autorité de protection des données.

TITRE III : DES OBLIGATIONS ET DU CONTROLE DU RESPONSABLE DE TRAITEMENT, DU SOUS-TRAITANT ET DE LEUR PREPOSÉ DANS LE TRAITEMENT DES DONNÉES À CARACTERE PERSONNEL

CHAPITRE I : DES OBLIGATIONS DE RESPONSABLES DU TRAITEMENT DE DONNEES A CARACTERE PERSONNEL

Article 221.

Le responsable du traitement ou son représentant est tenu de, notamment :

1. faire toute diligence pour tenir les données à jour de données inexactes, incomplètes, ou non pertinentes, ainsi que celles obtenues ou traitées en méconnaissance des dispositions du présent Livre;
2. veiller à ce que, pour les personnes agissant sous son autorité, l'accès aux données et les possibilités de traitement soient limités à ce dont ces personnes ont besoin pour l'exercice de leurs fonctions ou à ce qui est nécessaire pour les nécessités du service ;
3. informer les personnes agissant sous son autorité des dispositions du présent Livre et de ses mesures d'application, ainsi que de toute prescription pertinente, relative à la protection de la vie privée à l'égard des traitements des données à caractère personnel ;
4. s'assurer de la conformité des logiciels servant au traitement automatisé des données à caractère personnel avec les termes de la déclaration visée à l'article 388 ainsi que de la régularité de leur application ;
5. mettre en œuvre toutes les mesures techniques et l'organisation appropriées pour assurer la protection des données qu'il traite contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite ;
6. Assurer la formation de ses agents qui s'occupent au quotidien du traitement des données a caractère personnel ;
7. empêcher toute personne non autorisée d'accéder aux installations utilisées pour le traitement de données ;
8. empêcher que des supports de données puissent être lus, copiés, modifiés ou déplacés par une personne non autorisée ;
9. empêcher l'introduction non autorisée de toute donnée dans le système d'information, ainsi que toute prise de connaissance, toute modification ou tout effacement non autorisés de données enregistrées ;
10. empêcher que des systèmes de traitement de données soient utilisés à des fins de blanchiment de capitaux et de financement du terrorisme ;
11. empêcher que, lors de la communication de données et du transport de supports de données, les données puissent être lues, copiées, modifiées, altérées ou effacées de façon non autorisée ;

12. garantir que, lors de l'utilisation d'un système de traitement automatisé de données, les personnes autorisées ne puissent accéder qu'aux données relevant de leur autorisation ;
13. garantir que puisse être vérifiée et constatée l'identité des tiers auxquels des données peuvent être transmises par des installations de transmission ;
14. garantir que puisse être vérifiée et constatée a posteriori l'identité des personnes ayant eu accès au système d'information contenant des données à caractère personnel, la nature des données qui ont été introduites, modifiées, altérées, copiées, effacées ou lues dans le système, le moment auquel ces données ont été manipulées ;
15. sauvegarder les données par la constitution de copies de sécurité protégées.

Article 222.

Le responsable du traitement ou son représentant doit fournir à la personne dont les données font l'objet d'un traitement, au plus tard, lors de la collecte et quels que soient les moyens et supports employés, au moins les informations suivantes :

1. l'identité et les coordonnées du responsable du traitement et, le cas échéant, du représentant du responsable du traitement;
2. le cas échéant, les coordonnées du délégué à la protection des données ;
3. les finalités déterminées du traitement auquel les données sont destinées lorsque le traitement est fondé sur des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers ;
4. les catégories de données concernées ;
5. les destinataires auxquels les données sont susceptibles d'être communiquées ;
6. le fait de pouvoir demander à ne plus figurer sur le fichier ;
7. l'existence d'un droit de s'opposer, sur demande et gratuitement, au traitement de données à caractère personnel la concernant envisagé à des fins de prospection notamment commerciale, caritative ou politique ;
8. le caractère obligatoire ou non de la réponse, le caractère réglementaire ou contractuel ainsi que les conséquences éventuelles d'un défaut de réponse ;
9. l'existence d'un droit d'accès à l'information aux données la concernant et de demande de mise à jour de ses données ;
10. lorsque le traitement est fondé sur 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 l'Autorité ;
12. la durée de conservation des données ;

13. l'existence d'une prise de décision automatisée, y compris un profilage et, au moins en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée;
14. l'éventualité de tout transfert de données à destination d'Etats tiers.

Article 223.

Le responsable de traitement met en œuvre les moyens nécessaires de façon à garantir la sécurité des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, le backup et la restauration, Il est également civilement responsable sur les autres personnes traitant ces données.

Il met également en œuvre tous les moyens appropriés pour ne garantir que, par défaut, seules les données à caractère personnel nécessaires au regard de chaque finalité spécifique du traitement soient traitées.

Article 224.

Le responsable du traitement désigne un délégué à la protection des données à caractère personnel pour garantir que les traitements ne soient pas susceptibles de porter atteinte aux droits et libertés des personnes concernées. Le correspondant est chargé notamment :

1. d'assurer, d'une manière indépendante, l'application interne des dispositions du présent Livre ;
2. de tenir un registre des traitements effectués par le responsable du traitement, contenant les informations visées aux articles 398 et 399 de la présente loi.

Article 225.

Les données à caractère personnel sont traitées et ou stockées de manière confidentielle et protégée, notamment lorsque le traitement comporte des transmissions de données dans un réseau.

Article 226.

Lorsque le traitement est confié à un sous-traitant, le responsable du traitement ou, le cas échéant, son représentant en République Démocratique du Congo, doit :

1. se rassurer que le sous-traitant sélectionné remplit toutes conditions requises par la loi en vigueur sur la sous-traitance
2. se rassurer que le sous-traitant sélectionné, remplit les garanties suffisantes au regard des mesures de sécurité, éthique et d'organisation relatives aux traitements ainsi que les capacités techniques conformément aux lois en vigueur, notamment pour la mise en œuvre

des mesures de sécurité et de confidentialité, de manière à ce que le traitement réponde aux exigences du présent Livre et garantisse la protection des droits des personnes concernées ;

3. veiller au respect des mesures du point 1, ci-dessus, notamment par la stipulation de mentions spécifiques dans les contrats passés avec des sous-traitants ;
4. fixer dans le contrat, la responsabilité du sous- traitant à l'égard du responsable du traitement et les obligations incombant au sous-traitant en matière de protection de la sécurité et de la confidentialité des données ;
5. convenir avec le sous-traitant que celui-ci n'agit que sur la seule instruction du responsable du traitement et est tenu par les mêmes obligations que celles auxquelles le responsable du traitement est tenu ;
6. consigner par écrit ou sur un support électronique les éléments du contrat visés dans le présent article.

Article 227.

Le responsable du traitement veille à ce que le délégué à la protection des données 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 du traitement aide le délégué à la protection des données à exercer les missions visées à l'article 215 en fournissant les ressources nécessaires pour exercer ces missions, ainsi que l'accès aux données à caractère personnel et aux opérations de traitement, et lui permettant d'entretenir ses connaissances spécialisées.

Le responsable du traitement veille à ce que le délégué à la protection des données ne reçoive aucune instruction en ce qui concerne l'exercice de ses missions. Le délégué à la protection des données ne peut être relevé de ses fonctions ou pénalisé par le responsable du traitement ou le sous-traitant pour l'exercice de ses missions. Le délégué à la protection des données fait directement rapport au niveau le plus élevé de la direction du responsable du traitement ou du sous- traitant.

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

Le délégué à la protection des données est soumis au secret professionnel en ce qui concerne l'exercice de ses missions.

Le délégué à la protection des données peut exécuter d'autres missions et tâches. Le responsable du traitement ou le sous-traitant veillent à ce que ces missions et tâches n'entraînent pas de conflit d'intérêt.

Article 228.

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

1. informer et conseiller le responsable du traitement ou le sous-traitant ainsi que les employés qui procèdent au traitement sur les obligations qui leur incombent en vertu des dispositions du présent Livre en matière de protection des données ;
2. contrôler le respect des dispositions du présent Livre en matière de protection des données et des règles internes du responsable du traitement ou du sous-traitant en matière de protection des données à caractère personnel, y compris en ce qui concerne la répartition des responsabilités, la sensibilisation et la formation du personnel participant aux opérations de traitement, et les audits s'y rapportant ;
3. dispenser des conseils, sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données et vérifier l'exécution de celle-ci conformément aux dispositions du présent Livre ;
4. coopérer avec l'autorité ayant en charge la protection des données à caractère personnel ;
5. faire office de point focal pour l'autorité ayant en charge la protection des données à caractère personnel sur les questions relatives au traitement, y compris la consultation préalable conformément aux dispositions du présent Livre, et mener des consultations, le cas échéant, sur tout autre sujet.

Le délégué à la protection des données 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.

Article 229.

Chaque responsable du traitement tient un registre des activités de traitement effectuées sous leur responsabilité. Ce registre comporte toutes les informations suivantes :

1. le nom et les coordonnées du responsable du traitement et, le cas échéant, du responsable conjoint du traitement, du représentant du responsable du traitement et du délégué à la protection des données ;
2. les finalités du traitement ;
3. une description des catégories de personnes concernées et des catégories de données à caractère personnel ;
4. les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, y compris les destinataires dans des pays tiers ou des organisations internationales ;

5. le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale ;
6. les délais prévus pour l'effacement des différentes catégories de données ;
7. une description générale des mesures de sécurité techniques et organisationnelles.

Article 230.

Le responsable du traitement et, le cas échéant, leur représentant met le registre à la disposition de l'Autorité de protection des données.

Les obligations de tenir un registre et de designer un délégué ne s'appliquent pas aux petites et moyennes entreprises sauf si le traitement qu'elles effectuent est susceptible de comporter un risque pour les droits et les libertés des personnes concernées, s'il n'est pas occasionnel ou s'il porte notamment sur les catégories particulières de données ou sur des données à caractère personnel relatives à des condamnations pénales.

CHAPITRE II : DES OBLIGATIONS DU PREPOSE

Article 231.

Toute personne ayant accès aux données à caractère personnel et agissant sous l'autorité et le contrôle du responsable du traitement, est tenue de suivre les instructions de ce dernier pour traiter les données à caractère personnel.

CHAPITRE III : DES OBLIGATIONS DU SOUS-TRAITANT

Article 232.

Le sous-traitant est tenu de ne traiter les données que dans la limite du contrat qui le lie avec le Responsable de traitement.

Article 233.

Chaque sous-traitant tient un registre de toutes les catégories d'activités de traitement effectuées pour le compte du responsable du traitement, comprenant :

1. le nom et les coordonnées du ou des sous- traitants et de chaque responsable du traitement pour le compte duquel le sous-traitant agit ainsi que, le cas échéant, les noms et les coordonnées du représentant du responsable du traitement ou du sous-traitant et celles du délégué à la protection des données ;
2. les catégories de traitements effectués pour le compte de chaque responsable du traitement ;

3. le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts, les documents attestant de l'existence de garanties appropriées ;
4. une description générale des mesures de sécurité techniques et organisationnelles.

Les registres se présentent sous une forme écrite, y compris la forme électronique.

Article 234.

Le sous-traitant et, le cas échéant, son représentant met le registre à la disposition de l'Autorité de protection des données à caractère personnel sur demande.

Les obligations de tenir un registre et de designer un délégué ne s'appliquent pas aux petites et moyennes entreprises sauf si le traitement qu'elles effectuent est susceptible de comporter un risque pour les droits et les libertés des personnes concernées, s'il n'est pas occasionnel ou s'il porte notamment sur les catégories particulières ou sur des données à caractère personnel relatives à des condamnations pénales.

Article 235.

Sans préjudice du Livre III, les prestataires de services de confiance visés par le Livre précité sont soumis aux exigences aux exigences de protection des données à caractère personnel prévues par les dispositions du présent Livre.

CHAPITRE IV : DES DROITS DE LA PERSONNE CONCERNÉE

Article 236.

Toute personne physique dont les données à caractère personnel font l'objet d'un traitement peut demander au responsable de ce traitement :

1. les informations permettant de connaître et de contester le traitement de ses données à caractère personnel ;
2. la confirmation que des données à caractère personnel la concernant font ou ne font pas l'objet de traitement, ainsi que des informations portant au moins sur les finalités du traitement, les catégories de données sur lesquelles il porte et les catégories de destinataires auxquels les données sont communiquées ;
3. la communication sous forme intelligible des données à caractère personnel qui la concernent ainsi que de toute information disponible quant à l'origine de celles-ci ;
4. le cas échéant, des informations relatives aux transferts de données à caractère personnel envisagés à destination d'un État tiers, après avis de l'Autorité en charge de la Protection des données ;

5. lorsque cela est possible, la durée de conservation des données à caractère personnel envisagée ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée ;
6. l'existence du droit de demander au responsable du traitement la rectification ou l'effacement de données à caractère personnel, ou une limitation du traitement des données à caractère personnel relatives à la personne concernée, ou du droit de s'opposer à ce traitement ;
7. le droit d'introduire une réclamation auprès de l'Autorité compétente;
8. lorsque les données à caractère personnel ne sont pas collectées auprès de la personne concernée, toute information disponible quant à leur source.

Une copie des renseignements lui est communiquée au plus tard dans les soixante jours de la réception de la demande.

Le paiement des frais pour toute copie supplémentaire demandée par la personne concernée devra être fixé par note de service de la structure responsable du traitement sur la base des coûts administratifs conséquents.

Toutefois, l'Autorité de protection des données saisie contradictoirement par le responsable du fichier peut lui accorder :

1) des délais de réponse ;
2) l'autorisation de ne pas tenir compte de certaines demandes manifestement abusives par leur nombre, leur caractère répétitif ou systématique.

Lorsque les données relatives à la santé de la personne concernée sont traitées aux fins de recherches médico-scientifiques, 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 individuelle, la communication peut, pour autant qu'elle soit susceptible de nuire gravement auxdites recherches, être différée au plus tard jusqu'à l'achèvement des recherches. Dans ce cas, la personne concernée doit avoir préalablement donné son autorisation écrite au responsable du traitement que les données à caractère personnel la concernant peuvent être traitées à des fins médico-scientifiques et la communication de ces données peut dès lors être différée.

Article 237.

Les personnes concernées ont le droit de recevoir les données à caractère personnel les concernant qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par un support numérique ou autre format lisible, et ont le droit de transmettre ces données à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle, lorsque :

1) le traitement est fondé sur le consentement ou sur un contrat ; et
2) le traitement est effectué à l'aide de procédés automatisés.

Lorsque la personne concernée exerce son droit à la portabilité des données en application de l'alinéa premier du présent article, elle a le droit d'obtenir que les données à caractère personnel soient transmises directement d'un responsable du traitement à un autre, lorsque cela est techniquement possible.

Ce droit ne s'applique pas au traitement nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement.

Le droit visé à l'alinéa 1 du présent article ne porte pas atteinte aux droits et libertés de tiers.

Article 238.

Toute personne justifiant de son identité a le droit de contacter l'Autorité de protection des données en vue de savoir si les différents traitements effectués par les organes ou services compétents, portent sur des informations nominatives la concernant et, le cas échéant, d'en obtenir communication.

Article 239.

Toute personne physique a le droit de s'opposer, à tout moment, pour des motifs légitimes, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement.

Elle a le droit aussi, d'une part, d'être informée avant que des données la concernant ne soient pour la première fois communiquées à des tiers ou utilisées pour le compte de tiers à des fins de prospection notamment commerciale, caritative ou politique et, d'autre part, de se voir expressément offrir le droit de s'opposer, gratuitement, à ladite communication ou utilisation.

Ce droit doit être explicitement proposé à la personne concernée d'une façon intelligible et doit pouvoir être clairement distingué d'autres informations.

Lorsqu'il est fait droit à une opposition conformément à cet article, le responsable du traitement n'utilise ni ne traite plus les données à caractère personnel concernées.

Lorsque les données à caractère personnel sont collectées à des fins de prospection notamment commerciale, caritative ou politique, la personne concernée peut s'opposer, gratuitement et sans aucune justification, au traitement projeté de données à caractère personnel la concernant.

Pour exercer son droit d'opposition, l'intéressé adresse une demande datée et signée, par voie postale ou électronique, au responsable du traitement ou son représentant. Le responsable du traitement doit communiquer dans les trente jours qui suivent la réception de la demande prévue à l'alinéa précédent, quelle suite il a donnée à la demande de la personne concernée.

Lorsque des données à caractère personnel sont collectées par écrit, que ce soit sur un support papier, support numérique ou tout autre support équivalent, auprès de la personne concernée, le responsable du traitement demande, à celle-ci, sur le document grâce auquel il collecte ses données, si elle souhaite exercer le droit d'opposition.

En cas de contestation, la charge de la preuve incombe au responsable de traitement auprès duquel est exercé le droit d'accès sauf lorsqu'il est établi que les données contestées ont été communiquées par l'intéressé ou avec son accord.

Lorsque les données à caractère personnel sont collectées auprès de la personne concernée, autrement que par écrit, le responsable du 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 soixante jours 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 240.

Toute personne physique peut exiger du responsable du traitement que soient, selon les cas, et dans les meilleurs délais, mises à jour ou verrouillées les données à caractère personnel la concernant, qui sont inexactes, incomplètes, équivoques, périmées, non pertinentes ou dont la collecte, l'utilisation, la communication ou la conservation est interdite.

Pour exercer son droit de rectification ou de suppression, l'intéressé adresse une demande, par voie postale ou par voie électronique, datée et signée au responsable du traitement, ou son représentant.

Dans les trente jours qui suivent la réception de la demande prévue à l'alinéa précédent, le responsable du traitement communique les rectifications ou effacements des données effectués à la personne concernée elle-même ainsi qu'aux personnes à qui les données inexactes, incomplètes, équivoques, périmées, non pertinentes ou dont la collecte, l'utilisation, la communication ou la conservation est interdite, ont été communiquées. Quand le responsable du traitement n'a pas connaissance des destinataires de la communication et que la notification à ces destinataires ne paraît pas possible ou implique des efforts disproportionnés, il le leur notifie dans le délai imparti.

En cas de non-respect du délai prévu à l'alinéa précédent, une plainte peut être adressée à l'autorité ayant en charge la protection des données à caractère personnel par l'auteur de la demande.

Si une information a été transmise à un tiers, sa rectification ou son annulation doit être notifiée à ce tiers, sauf dispense accordée par l'autorité ayant en charge la protection des données à caractère personnel.

Les ayants droit d'un de cujus justifiant de leur identité peuvent, si des éléments portés à leur connaissance leur laissent présumer que les données à caractère personnel le concernant faisant l'objet d'un traitement n'ont pas été actualisées, exiger du responsable de ce traitement qu'il prenne en considération le décès et procède aux mises à jour qui doivent en être la conséquence.

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

Article 241.

La personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant et le responsable du traitement a l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais, 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. les données à caractère personnel doivent être effacées pour respecter une obligation légale qui est prévue auquel le responsable du traitement est soumis;
3. pour respecter une obligation légale qui requiert le traitement prévue par le auquel le responsable du 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 du traitement;

Article 242.

Lorsque le responsable du traitement a rendu publiques les données à caractère personnel de la personne concernée, il prend toutes les mesures raisonnables, y compris les mesures techniques, en ce qui concerne les données publiées sous sa responsabilité, en vue d'informer les tiers qui traitent lesdites données qu'une personne concernée leur demande d'effacer tout lien vers ces données à caractère personnel, ou toute copie ou reproduction de celles-ci.

Lorsque le responsable du 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'oubli numérique et à l'effacement des données à caractère personnel.

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

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

Les alinéas 1, 2, 3 et 4 ne s'appliquent pas dans la mesure où ce traitement est nécessaire :

1) à l'exercice du droit à la liberté d'expression et d'information ;
2) pour respecter une obligation légale qui requiert le traitement ou pour exécuter une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ;
3) pour des motifs d'intérêt public dans le domaine de la santé publique ;
4) à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques dans la mesure où le droit visé à l'alinéa 1er 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.

Article 243.

L'Autorité de protection des données adopte, sans préjudice des dispositions du présent Livre, des mesures ou des lignes directrices aux fins de préciser :

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

Article 244.

En ce qui concerne les traitements relatifs à la sûreté de l'Etat, la défense et la sécurité publique, la demande est adressée à l'Autorité de protection des données qui désigne l'un de ses membres pour mener toutes investigations utiles et faire procéder aux modifications nécessaires. Celui-ci peut se faire assister d'un autre membre de ladite autorité.

Il est notifié au requérant qu'il a été procédé aux vérifications.

Lorsque l'Autorité de protection des données constate, en accord avec le responsable du traitement, que la communication des données qui y sont contenues ne met pas en cause ses finalités, la sûreté de l'État, la défense ou la sécurité publique, ces données peuvent être communiquées au requérant.

Lorsque le traitement est susceptible de comprendre des informations dont la communication ne mettrait pas en cause les fins qui lui sont assignées, l'Autorité de protection des données peut prévoir que ces informations peuvent être communiquées au requérant par le gestionnaire du fichier directement saisi dans un délai de trente jours suivant la réception de la demande.

CHAPITRE V : DU CONTROLE DU TRAITEMENT DES DONNÉES À CARACTERE PERSONNEL

Article 245.

Le contrôle de traitements à caractère personnel effectués par un responsable de traitement ou son délégué, le sous-traitant ainsi que les sanctions administratives de leur non-conformité au présent Livre, sont de la compétence exclusive de l'Autorité de protection des données.

Cette prérogative ne peut être déléguée à un organe tiers, sauf si l'organe a :

1. démontré, à la satisfaction de protection des données à caractère personnel, son indépendance et son expertise ;
2. établi des procédures qui lui permettent d'apprécier si les responsables du traitement et les sous-traitants concernés satisfont aux conditions de contrôler le respect des dispositions et d'examiner périodiquement son fonctionnement ;
3. établi des procédures et des structures pour traiter les réclamations relatives aux violations par un responsable du traitement ou un sous-traitant ;
4. démontré, à la satisfaction de l'autorité ayant en charge la protection des données à caractère personnel, que ses tâches et ses missions n'entraînent pas de conflit d'intérêt.

L'Autorité de protection des données révoque l'agrément de l'organe si les conditions d'agrément ne sont pas ou ne sont plus réunies ou si les mesures prises par l'organe constituent une violation des dispositions du présent Livre.

Article 246.

Lorsque les données à caractère personnel n'ont pas été collectées auprès de la personne concernée, le responsable du traitement ou son représentant fournit, dès l'enregistrement des données ou, si une communication de données à un tiers est envisagée, au plus tard au moment de la première communication des données, à la personne concernée, sauf si elle en est déjà informée :

1) l'identité et les coordonnées du responsable du traitement et, le cas échéant, du délégué à la protection des données
2) les finalités du traitement ;
3) l'existence d'un droit de s'opposer, sur demande et gratuitement, au traitement de données à caractère personnel la concernant à des fins de prospection directe notamment commerciale, caritative ou politique. Dans ce cas, la personne concernée est informée avant que des données à caractère personnel ne soient pour la première fois communiquées à des tiers ou utilisées pour le compte de tiers à des fins de prospection ;
4) d'autres informations supplémentaires suivantes :
   - les catégories de données concernées ;
   - les destinataires ou les catégories de destinataires ;

- la durée de conservation des données ;
- l'éventualité de tout transfert de données à destination d'Etats tiers, lorsque le traitement est fondé sur les intérêts légitimes poursuivis par le responsable du traitement ou par un tiers ;
- l'existence d'un droit d'accès aux données la concernant et de rectification ou d'effacement de ces données ;
- lorsque le traitement est fondé sur 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 ;
- le droit d'introduire une réclamation auprès de l'Autorité ;
- la source d'où proviennent les données à caractère personnel et, le cas, échéant, une mention indiquant qu'elles sont issues de sources accessibles au public ;
- l'existence d'une prise de décision automatisée, y compris un profilage et, au moins en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée.

Le responsable du traitement fournit les informations visées à l'alinéa premier :

1) dans un délai raisonnable après avoir obtenu les données à caractère personnel, mais ne dépassant pas trente jours, eu égard aux 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 ladite personne ; ou
3) s'il est envisagé de communiquer les informations à un autre destinataire, au plus tard lorsque les données à caractère personnel sont 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 du traitement fournit au préalable à la personne concernée des informations au sujet de cette autre finalité et toute autre information pertinente visée à l'alinéa 1er.

Article 247.

Conformément aux dispositions du présent Livre, le responsable du traitement est dispensé de fournir les informations lorsque :

1. en particulier pour un traitement à des fins statistiques, historiques ou scientifiques ou pour le dépistage motivé par la protection et la promotion de la santé publique, l'information de la personne concernée se révèle impossible ou implique des efforts disproportionnés ;
2. la personne concernée dispose déjà de ces informations ;
3. l'enregistrement ou la communication des données à caractère personnel est effectué en vue de l'application d'une disposition d'une loi ou d'un décret.

Article 248.

Le responsable du traitement prend des mesures appropriées pour fournir toute information ainsi que pour procéder à toute communication, en ce qui concerne le traitement à la personne concernée d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples, en particulier pour toute information destinée spécifiquement à un enfant.

Les informations sont fournies par écrit ou par d'autres moyens y compris, lorsque c'est approprié, par voie électronique.

Toutefois, la personne concernée peut faire une demande écrite ; dans ce cas les informations lui seront fournies par écrit également, à condition que l'identité de la personne concernée soit démontrée par d'autres moyens.

Article 249.

Le responsable du traitement facilite l'exercice des droits conférés à la personne concernée. Dans ce cas, le responsable du traitement ne refuse pas de donner suite à la demande de la personne concernée d'exercer les droits que lui confèrent le présent Livre, à moins que le responsable du traitement ne démontre qu'il n'est pas en mesure d'identifier la personne concernée.

Article 250.

Le responsable du traitement fournit à la personne concernée des informations sur les mesures prises à la suite d'une demande formulé dans les meilleurs délais et en tout état de cause dans un délai de trente jours à compter de la réception de la demande. Au besoin, ce délai peut être prolongé de soixante jours, compte tenu de la complexité et du nombre de demandes.

Le responsable du traitement informe la personne concernée de cette prolongation et des motifs du report dans un délai de trente jours à compter de la réception de la demande.

Lorsque la personne concernée présente sa demande sous une forme électronique, les informations sont fournies par voie électronique lorsque cela est possible, à moins que la personne concernée ne demande qu'il en soit autrement.

Si le responsable du traitement ne donne pas suite à la demande formulée par la personne concernée, il informe celle-ci sans tarder et au plus tard dans un délai de trente jours à compter de la réception de la demande des motifs de son inaction.

La personne concernée à la possibilité d'introduire une réclamation auprès de l'autorité ayant en charge la protection des données à caractère personnel et de former un recours juridictionnel.

Article 251.

Aucun paiement n'est exigé pour fournir les informations et pour procéder à toute communication et prendre toute mesure.

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

1) 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
2) refuser de donner suite à ces demandes. Il incombe au responsable du traitement de démontrer le caractère manifestement infondé ou excessif de la demande.

Article 252.

Sans préjudice des dispositions relatives à la protection des données personnelles des condamnations pénales, et aux mesures de sécurité connexes, lorsque le responsable du traitement a des doutes raisonnables quant à l'identité de la personne physique présentant la demande particulière, il peut demander que lui soient fournies des informations supplémentaires nécessaires pour confirmer l'identité de la personne concernée.

Article 253.

Les informations à communiquer aux personnes peuvent être fournies accompagnées d'icônes normalisées afin d'offrir une bonne vue d'ensemble, facilement visible, compréhensible et clairement lisible, du traitement prévu. Lorsque les icônes sont présentées par voie électronique, elles sont lisibles par machine.

Article 254.

Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques, le responsable du 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, tels que la minimisation des données, de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent Livre et de protéger les droits de la personne concernée.

Le responsable du 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. Ces mesures

s'appliquent à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de 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 sans l'intervention de la personne physique concernée.

Article 255.

Le responsable du traitement doit notifier, sans délai, à l'Autorité de protection des données et à la personne concernée toute rupture de la sécurité ayant affecté les données à caractère personnel de la personne concernée.

Le sous-traitant doit avertir, sans délai, le responsable du traitement de toute rupture de la sécurité ayant affecté les données à caractère personnel qu'il traite pour le compte et au nom du responsable du traitement.

La notification visée à l'alinéa 1 doit, à la limite :

1) décrire la nature de la rupture de sécurité ayant affecté des données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la rupture et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;
2) communiquer le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
3) décrire les conséquences probables de la rupture de sécurité ;
4) décrire les mesures prises ou que le responsable du traitement propose de prendre pour remédier à la rupture de sécurité, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

La communication à la personne concernée visée à l'alinéa 1 n'est pas nécessaire si l'une ou l'autre des conditions suivantes est remplie :

1) le responsable du 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 ladite rupture, 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 du traitement a pris des mesures ultérieures qui garantissent que le risque élevé pour les droits et libertés des personnes concernées visé à l'alinéa 1er 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.

Article 256.

Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel. Une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires.

Lorsqu'il effectue une analyse d'impact relative à la protection des données, le responsable du traitement demande conseil au délégué à la protection des données, si un tel délégué a été désigné.

L'analyse d'impact relative à la protection des données visée à l'alinéa 1 est, en particulier, requise dans les cas suivants :

1) l'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire ; ou
2) la surveillance systématique à grande échelle d'une zone accessible au public.

L'Autorité de protection des données établit et publie une liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise conformément à l'alinéa 1.

Elle peut aussi établir et publier une liste des types d'opérations de traitement pour lesquelles aucune analyse d'impact relative à la protection des données n'est requise.

L'analyse contient au moins :

1) une description systématique des opérations de traitement envisagées et des finalités du traitement, y compris, le cas échéant, l'intérêt légitime poursuivi par le responsable du traitement ;
2) une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités ;
3) une évaluation des risques pour les droits et libertés des personnes concernées conformément à l'alinéa 1 ; et
4) les mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect des dispositions du présent Livre, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées.

Le cas échéant, le responsable du traitement demande l'avis des personnes concernées ou de leurs représentants au sujet du traitement prévu, sans préjudice de la protection des intérêts généraux ou commerciaux ou de la sécurité des opérations de traitement.

Si nécessaire, le responsable du traitement procède à un examen afin d'évaluer si le traitement est effectué conformément à l'analyse d'impact relative à la protection des données, au moins quand il se produit une modification du risque présenté par les opérations de traitement.

Article 257.

Le responsable du traitement consulte l'Autorité de protection des données préalablement au traitement lorsqu'une analyse d'impact relative à la protection des données effectuée au titre de l'article précédent indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque.

Lorsque l'Autorité de protection des données est d'avis que le traitement envisagé visé à l'alinéa 1, constituerait une violation des dispositions du présent Livre, en particulier lorsque le responsable du traitement n'a pas suffisamment identifié ou atténué le risque, l'Autorité de protection des données fournit par écrit, dans un délai maximum de huit semaines à compter de la réception de la demande de consultation, un avis écrit au responsable du traitement et, le cas échéant, au sous-traitant, et peut faire usage de ses pouvoirs. Ce délai peut être prolongé de quatre semaines, en fonction de la complexité du traitement envisagé. L'Autorité de protection des données informe le responsable du traitement et, le cas échéant, le sous-traitant de la prolongation du délai ainsi que des motifs du retard, dans un délai de quinze jours à compter de la réception de la demande de consultation. Ces délais peuvent être suspendus jusqu'à ce que l'Autorité de protection des données ait obtenu les informations qu'elle a demandées pour les besoins de la consultation.

Lorsque le responsable du traitement consulte l'Autorité de protection des données en application de l'alinéa 1, il lui communique :

1) le cas échéant, les responsabilités respectives du responsable du traitement, des responsables conjoints et des sous-traitants participant au traitement, en particulier pour le traitement au sein d'un groupe d'entreprises ;
2) les finalités et les moyens du traitement envisagé ;
3) les mesures et les garanties prévues afin de protéger les droits et libertés des personnes concernées en vertu des dispositions du présent Livre ;
4) le cas échéant, les coordonnées du délégué à la protection des données ;
5) l'analyse d'impact relative à la protection des données prévue à l'article précédent ;
6) et toute autre information que l'Autorité de protection des données demande.

Article 258.

Lorsque l'article 222 s'applique en ce qui concerne l'offre directe de services de la société de l'information aux mineurs, le traitement des données à caractère personnel relatives à un mineur n'est licite que dans la mesure où, le consentement est donné par le titulaire de la responsabilité parentale à l'égard du mineur.

Le responsable du traitement s'efforce raisonnablement de vérifier, en pareil cas, que le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant, compte tenu des moyens technologiques disponibles.

Article 259.

En cas d'incapacité d'un majeur au sens du code de la famille dûment attestée par un professionnel des soins de santé, les droits, tels que fixés par les dispositions du présent Livre, d'une personne concernée majeure, sont exercés par le ou la conjoint(e) cohabitant(e) ou toute personne commise à la protection des intérêts de ce majeur conformément au code de la famille.

La personne concernée est associée à l'exercice de ses droits autant qu'il est possible et compte tenu de sa capacité de compréhension.

Article 260.

Sans préjudice de tout autre recours administratif ou juridictionnel, toute personne concernée a le droit d'introduire une réclamation auprès de l'Autorité de protection des données, si elle considère que le traitement de données à caractère personnel la concernant constitue une violation des dispositions du présent Livre.

L'Autorité de protection des données informe l'auteur de la réclamation de l'état d'avancement et de l'issue de la réclamation, y compris de la possibilité d'un recours juridictionnel en vertu de l'article suivant.

Article 261.

Toute personne concernée a le droit de former un recours effectif devant la juridiction administrative compétente lorsque l'autorité ayant en charge la protection des données à caractère personnel ne traite pas une réclamation ou n'informe pas la personne concernée, dans un délai de soixante jours, de l'état d'avancement ou de l'issue de la réclamation qu'elle a introduite au titre de l'article précédent.

Article 262.

Toute personne concernée a droit à un recours juridictionnel effectif devant le tribunal de paix de son ressort si elle considère que les droits que lui confèrent les dispositions du présent Livre

ont été violés du fait d'un traitement de ses données à caractère personnel effectué en violation des dispositions du présent livre.

Article 263.

Toute personne ayant subi un dommage matériel ou moral du fait d'une violation des dispositions du présent Livre a le droit d'obtenir du responsable du traitement ou du sous-traitant réparation du préjudice subi.

Tout responsable du traitement ayant participé au traitement est responsable du dommage causé par le traitement qui constitue une violation des dispositions du présent Livre. Un sous-traitant n'est tenu pour responsable du dommage causé par le traitement que s'il n'a pas respecté les obligations prévues par les dispositions du présent Livre qui incombent spécifiquement aux sous-traitants ou qu'il a agi en dehors des instructions licites du responsable du traitement ou contrairement à celles-ci.

Un responsable du traitement ou un sous-traitant est exonéré de responsabilité, au titre de l'alinéa 2, s'il prouve que le fait qui a provoqué le dommage ne lui est nullement imputable.

Lorsque plusieurs responsables du traitement ou sous-traitants ou lorsque, à la fois, un responsable du traitement et un sous-traitant participent au même traitement et, lorsque, au titre des alinéas 2 et 3, ils sont responsables d'un dommage causé par le traitement, chacun des responsables du traitement ou des sous-traitants est tenu solidairement responsable du dommage (dans sa totalité) afin de garantir à la personne concernée une réparation effective.

Lorsqu'un responsable du traitement ou un sous-traitant a, conformément à l'alinéa 4, réparé totalement le dommage subi, il est en droit de réclamer auprès des autres responsables du traitement ou sous-traitants ayant participé au même traitement la part de la réparation correspondant à leur part de responsabilité dans le dommage, conformément aux conditions fixées à l'alinéa 2.

Les actions judiciaires engagées pour exercer le droit à obtenir réparation sont intentées devant les juridictions compétentes.

Article 264.

Les responsables conjoints du 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 des informations, par voie d'accord entre eux. Un point de contact pour les personnes concernées peut être désigné dans l'accord.

L'accord visé à l'alinéa 1 reflète dûment les rôles respectifs des responsables conjoints du traitement et leurs relations vis-à-vis des personnes concernées. Les grandes lignes de l'accord sont mises à la disposition de la personne concernée.

Indépendamment des termes de l'accord visé à l'alinéa 1, le Chapitre II : le concerné peut exercer les droits que lui confère les dispositions du présent Livre à l'égard de et contre chacun des responsables du traitement.

Article 265.

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

CHAPITRE V : DES DONNÉES PERSONNELLES SOUMISES A DES REGIMES PARTICULIERS

Article 266.

Les traitements de données à caractère personnel relatives aux infractions, aux condamnations pénales et aux mesures de sûreté connexes sont interdits. Ils peuvent uniquement être mis en œuvre par :

1. les juridictions, les autorités publiques et les personnes morales gérant un service public dans le cadre de leurs attributions légales, notamment leurs missions de police judiciaire ou administrative ;
2. les auxiliaires de justice, pour les stricts besoins de l'exercice des missions qui leur sont confiées par les dispositions légales et règlementaires notamment par des avocats ou d'autres conseils juridiques, pour autant que la défense de leurs clients l'exige ;
3. par d'autres personnes lorsque le traitement est nécessaire à la réalisation de finalités fixées par ou en vertu d'une disposition légale ou règlementaire ;
4. par des personnes physiques ou par des personnes morales de droit public ou de droit privé pour autant que la gestion de leurs propres contentieux l'exige.

Un registre complet des condamnations pénales ne peut être tenu que sous le contrôle de l'Autorité de protection des données.

Les personnes visées susceptibles de traiter les données à caractère personnel relatives aux condamnations pénales et aux mesures de sûreté connexes sont soumises au secret professionnel.

Article 267.

Le traitement ultérieur de données à caractère personnel à des fins historiques, statistiques ou scientifiques est interdit.

L'interdiction de traiter les données à caractère personnel visées à l'alinéa 1er ne s'applique pas dans les cas suivants :

1) l'objectif de la recherche ne peut être raisonnablement atteint sans que ces informations soient fournies sous une forme permettant d'identifier l'individu;
2) les informations sont divulguées à la condition qu'elles ne soient pas utilisées afin de contacter une personne pour participer à une étude ;
3) le lien enregistré ne porte pas préjudice à la personne concernée et les avantages découlant du lien enregistré relèvent clairement de l'intérêt public ;
4) le responsable du traitement concerné a approuvé l'ensemble des conditions relatives :
   - à la sécurité et confidentialité ;
   - au retrait ou destruction des identifiants individuels le plus tôt possible ;
   - à l'interdiction de toute utilisation ou divulgation ultérieure de ces informations sous une forme permettant d'identifier les individus sans l'autorisation expresse du responsable du traitement.
5) la personne à laquelle ces informations sont communiquées a signé un contrat l'engageant à respecter les conditions approuvées, les dispositions du présent Livre, les politiques et les procédures du responsable du traitement relatives à la confidentialité des informations à caractère personnel.

Le traitement ultérieur de données à caractère personnel à des fins historiques, statistiques ou scientifiques effectué à l'aide de données anonymes est admis.

Article 268.

Si les finalités pour lesquelles des données à caractère personnel sont traitées n'imposent pas ou n'imposent plus au responsable du 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 les cas visés à l'alinéa 1 du présent article, le responsable du 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. En pareil cas, les articles 223, 224, 227 et 228 ne sont pas applicables, sauf lorsque la personne concernée fournit, aux fins d'exercer les droits que lui confèrent ces articles, des informations complémentaires qui permettent de l'identifier.

Article 269.

Lors du traitement de données à caractère personnel visées aux articles du chapitre 5 du présent titre, le responsable du traitement doit prendre les mesures supplémentaires suivantes :

1) les catégories de personnes, ayant accès aux données à caractère personnel, doivent être désignées par le responsable du traitement ou, le cas échéant, par le sous-traitant, avec une description précise de leur fonction par rapport au traitement des données visées ;
2) la liste des catégories des personnes ainsi désignées doit être tenue à la disposition de l'Autorité de protection des données par le responsable du traitement ou, le cas échéant, par le sous-traitant ;
3) il doit veiller à ce que les personnes désignées soient tenues, par une obligation légale ou statutaire, ou par une disposition contractuelle équivalente, au respect du caractère confidentiel des données visées ;
4) lorsque l'information, due en vertu du présent Code, est communiquée à la personne concernée ou lors de la déclaration, le responsable du traitement doit mentionner la base légale ou réglementaire autorisant le traitement de données à caractère personnel visées aux articles du chapitre 5 du présent titre.

Article 270.

Lorsque le traitement de données à caractère personnel est exclusivement autorisé par le consentement écrit que ce soit sur support papier, support électronique ou tout autre support équivalent, de la personne concernée, le responsable du traitement doit préalablement communiqué, à la personne concernée, en sus des informations en vertu des dispositions du présent livre, les motifs pour lesquels ces données sont traitées, ainsi que la liste des catégories de personnes ayant accès aux données à caractère personnel.

Article 271.

Le responsable du traitement ou le sous-traitant informe la personne concernée de la possibilité de définir les modalités de la gestion de ses données à caractère personnel après sa mort.

A cet effet, la personne concernée indique les modalités relatives à la conservation, à l'effacement, à la communication et, s'il échet, à la transmission à une personne de son choix.

La personne concernée formule soit les directives d'ordre général qui concernent l'ensemble de ses données à caractère personnel soit les directives d'ordre spécial qui concernent qu'une partie de ses données à caractère personnel.

En cas d'absence des directives de la personne concernée, les héritiers de la personne concernée peuvent à tout moment entamer les processus de se faire communiquer les droits y afférents ou le cas échéant, se faire transmettre les données concernant le défunt.

TITRE V : DES MESURES ADMINISTRATIVES ET SANCTIONS

CHAPITRE I : DES MESURES ADMINISTRATIVES

Article 272.

Constitue des manquements, au titre du présent Livre, le fait de :

1. procéder à une collecte déloyale de données à caractère personnel ;
2. communiquer à un tiers non autorisé des données à caractère personnel ;
3. procéder à la collecte de données sensibles, de données relatives à des infractions ou à un numéro national d'identification sans respecter les conditions légales ;
4. procéder à la collecte ou à l'utilisation de données à caractère personnel ayant pour conséquence de provoquer une atteinte grave aux droits fondamentaux ou à l'intimité de la vie privée de la personne physique concernée ;
5. empêcher les services de l'Autorité de protection des données d'effectuer une mission de contrôle sur place ou faire preuve d'obstruction lors de la réalisation d'une telle mission.

Article 273.

L'Autorité de protection des données peut prononcer un avertissement à l'encontre du responsable du traitement qui ne respecte pas les obligations découlant des dispositions du présent Livre.

Elle peut également mettre en demeure le responsable du traitement de faire cesser le manquement constaté dans un délai fixé qui ne peut excéder huit jours.

Article 274.

Lorsque le responsable du traitement ne se conforme pas à la mise en demeure à se conformer aux dispositions du présent Livre, l'Autorité de protection des données peut prononcer à son encontre, dans le respect du principe du contradictoire, les sanctions suivantes :

1. injonction de cesser le traitement des données à caractère personnel, si la violation a mis en danger la sécurité et sûreté nationale et/ou conduit à un meurtre de masse, à un génocide ;
2. paiement de 5% de son chiffre d'affaires hors taxe de l'exercice écoulé, si la violation a conduit à la mort ou tentative de mort d'un ou plusieurs personnes ;
3. paiement de huit millions à deux cents millions de franc congolais si la violation n'a eu aucun impact grave sur l'État et/ou les personnes concernées.

L'État se garde le droit d'intenter une action pénale contre le responsable de traitement et de réclamer un dommage-intérêt pour lui et les personnes concernées.

Article 275.

Toute sanction prononcée par l'Autorité de protection des données peut être assortie d'une injonction de procéder, dans un délai qui ne peut excéder huit jours, à toute modification ou suppression utile dans le fonctionnement des traitements de données à caractère personnel, objet de la sanction.

Article 276.

Les sanctions prévues dans les dispositions du présent Livre sont prononcées sur la base d'un rapport établi par l'Autorité de protection des données. Ce rapport est notifié au responsable du traitement, qui peut faire des observations écrites ou orales dans un délai de quinze jours dès la réception de la notification de l'Autorité de protection des données et qui peut être assisté ou se faire représenter aux séances de travail à l'issue desquelles l'Autorité de protection des données statue.

Les décisions prises par l'Autorité de protection des données sont motivées et notifiées au responsable du traitement.

Article 277.

Les décisions prononçant une sanction peuvent faire l'objet d'un recours devant la juridiction administrative compétente.

Article 278.

Les sanctions prononcées peuvent être rendues publiques par l'Autorité de protection des données.

CHAPITRE II : DES SANCTIONS

Article 279.

Constituent des infractions au sens des dispositions du présent Livre, sans préjudice de celles prévues par le code pénal :

1. le fait d'entraver l'action de l'Autorité de protection des données :
    - en s'opposant à l'exercice des missions confiées à ses membres ou aux agents habilités ;

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

2. toute personne physique ou morale qui, sans droit, même par négligence, procède ou fait procéder à des traitements de données à caractère personnel sans avoir respecté les formalités préalables à leur mise en œuvre telles que prescrites par les dispositions du présent Livre ;
3. quiconque en connaissance de cause, décide de faire usage de données à caractère personnel collectées par le procédé décrit au point (2) ci-dessus, sans en être l'auteur est également condamné comme s'il était l'auteur du traitement frauduleux ;
4. le fait, hors les cas où le traitement des données a été réalisé dans les conditions prévues par les dispositions des dispositions du présent Livre, de procéder ou de faire procéder à un traitement de données à caractère personnel parmi lesquelles, des données sensibles relatives à des infractions ou des données relatives au numéro d'identification national ;
5. le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans avoir mis en œuvre les mesures prescrites par les dispositions du présent Livre ;
6. le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite ;
7. le fait pour 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 et/ou de manipuler ces informations ;
8. quiconque a transféré, fait ou laissé transférer des données à caractère personnel vers un État tiers sans qu'il ait été satisfait aux exigences prévues dans le présent Livre ;
9. quiconque, pour contraindre une personne à lui communiquer les renseignements obtenus par l'exercice du droit consacré par l'article 222 du présent Code, ou à donner son autorisation au traitement de données à caractère personnel la concernant, a usé à son égard de voies de fait, de violence ou menaces, de dons ou de promesses ;
10. le fait de procéder à un traitement des données à caractère personnel concernant une personne physique malgré la demande de rectification ou l'opposition de cette personne, lorsque cette demande de rectification ou cette opposition est fondée sur des motifs légitimes ;
11. le fait de ne pas respecter les dispositions du présent Livre relatives à l'information des personnes ;

12. le fait de ne pas respecter les dispositions du présent Livre relatives aux droits d'accès ;
13. le fait de conserver des données à caractère personnel au-delà de la durée prévue pour la déclaration préalable adressée à l'Autorité de protection des données sauf si cette conservation est effectuée à des fins historiques, statistiques ou scientifiques au sens du présent Livre;
14. 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 l'intéressé ou à l'intimité de sa vie privée, de porter sans autorisation de l'intéressé ces données à la connaissance d'un tiers qui n'a pas qualité pour les recevoir ;
15. le fait de participer à une association formée ou à une entente établie en vue de la commission d'une ou plusieurs infractions prévues par les dispositions du présent Livre.

Article 280.

Les infractions visées à l'article 269 le présent Code sont punies d'une peine de servitude pénale principale de six mois à dix ans et d'une amende de dix millions à cinquante millions de francs Congolais ou de l'une de ces deux peines seulement.

La complicité et la tentative sont punies des mêmes peines.

Si l'auteur de l'infraction au point 1 de l'article 269 procède ou fait procéder, par simple négligence, à des traitements de données à caractère personnel sans avoir respecté les formalités préalables à leur mise en œuvre telles que prescrites par les dispositions du présent Livre, seule une amende de cinq millions à cinquante millions de Francs congolais lui est appliquée.

Le tribunal peut ordonner l'effacement de tout ou partie des données à caractère personnel faisant l'objet du traitement ayant donné lieu à l'infraction.

Les décisions de condamnation devenues définitives prises en vertu de ce chapitre sont publiées dans le Journal officiel de la République Démocratique du Congo ainsi que sur un support électronique aux frais du condamné.

En cas de condamnation pour une des infractions prévues à l'article 269 du présent Code, la juridiction de jugement peut prononcer des peines à titre complémentaire.

Elle peut prononcer la confiscation des supports matériels des données à caractère personnel formant l'objet de l'infraction, tels que les fichiers manuels, disques et bandes magnétiques, à l'exclusion des ordinateurs ou de tout autre matériel, ou ordonner l'effacement de ces données

ainsi que des sommes, avantages ou produits résultant de l'infraction et appartenant au condamné.

La confiscation ou l'effacement peut être ordonné même si les supports matériels des données à caractère personnel n'appartiennent pas au condamné.

Les objets confisqués doivent être détruits lorsque la décision est passée en force de chose jugée.

Sans préjudice des interdictions énoncées par des dispositions particulières, en cas de condamnation pour une des infractions prévues à l'article 269 de du présent Code, la juridiction de jugement peut prononcer l'interdiction à titre de peine complémentaire. Cette interdiction implique une interdiction de gérer, personnellement ou par personne interposée, et pour deux ans au maximum, tout traitement de données à caractère personnel.

Toute infraction à l'interdiction édictée par l'alinéa 10 ou toute récidive relative aux infractions visées dans le présent chapitre sont punies d'une peine de servitude pénale d'un an à dix ans et d'une amende de dix millions à cent millions de Francs congolais ou de l'une de ces deux peines seulement.

Le présent article n'empêchera pas l'adoption de toute mesure d'indulgence établie par les dispositions du présent Livre, comme la suspension ou une peine avec sursis, sauf pour les décisions visées aux alinéas 5 à 10.

Le responsable de traitement ou son représentant sera passible du paiement des amendes encourues par son sous-traitant.

LIVRE VI : DE LA CYBERSECURITE ET DE LA CYBERCRIMINALITE

TITRE I : DE L'OBJET ET DU CHAMP D'APPLICATION

Article 281.

Les dispositions du présent Livre fixent les règles relatives à la cybersécurité et à la lutte contre la cybercriminalité.

Article 282.

Le présent Livre s'applique :

1. aux moyens permettant d'assurer la protection et l'intégrité des données numériques ;
2. aux infractions spécifiques liées aux technologies de l'information et de la communication, ainsi qu'à celles dont la commission est facilitée ou liée à l'utilisation de ces technologies ;

3. au cadre institutionnel et aux règles procédurales spécifiques à la cybersécurité et à la cybercriminalité en République Démocratique du Congo.

Article 283.

Les dispositions du présent livre ne s'appliquent pas :

- aux moyens de cryptologie utilisés par les missions diplomatiques et consulaires conformément aux traités et conventions régulièrement ratifiés ainsi que ceux relatifs à la sécurité intérieure et extérieure ;
- aux applications informatiques utilisées par les services spécialisés de défense et de sécurité nationale de la République Démocratique du Congo.

TITRE II : DU CADRE INSTITUTIONNEL

Article 284.

Le cadre institutionnel du secteur de la cybersécurité et celui de la cybercriminalité comprend :

1. La Direction Générale de la Sécurité des Systèmes d'Information ;
2. L'Agence National de lutte contre la cybercriminalité ;

CHAPITRE I : DE DIRECTION GÉNÉRALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

Article 285.

Il est créé par décret du Premier Ministre, délibéré en Conseil des Ministres, un organisme public dénommé « Direction Générale de Sécurité des Systèmes d'Information», en sigle «DGSSI», et placé sous l'autorité du Président de la République.

Article 286.

La DGSSI collabore notamment avec le Ministère ayant la défense nationale dans ses attributions et celui ayant numérique dans ses attributions ainsi que les services de sécurité.

La DGSSI est l'autorité nationale de régulation des activités de sécurité des systèmes informatiques. Elle est chargée d'accompagner et de sécuriser les systèmes d'information au profit du développement du secteur du numérique sur l'ensemble du territoire national.

Acteur majeur de la cybersécurité, l'ANSSI apporte son expertise et son assistance technique aux administrations ainsi qu'aux entreprises tant publiques que privées, avec une mission renforcée au profit des opérateurs d'importance vitale (OIV).

L'ANSSI apporte son expertise et son assistance technique aux administrations et aux entreprises publiques et privées.

Elle assure pour le compte de l'Etat, la régulation, le contrôle et le suivi des activités liées à la sécurité des systèmes d'information et des réseaux de communications électroniques et à la certification électronique.

Article 287.

L'ANSSI a pour mission de :

1. instruire les demandes d'homologation des moyens de cryptographie et cryptanalyse et de délivrer les certificats d'homologation des équipements de sécurité ;
2. participer à l'élaboration de la politique nationale de sécurité des réseaux et veiller à son exécution ;
3. contrôler les activités de sécurité des réseaux de communications électronique, des systèmes d'information et de certification ;
4. suivre l'exécution des plans et des programmes relatifs à la sécurité des systèmes d'information et des réseaux dans les secteurs public et privé et assurer la coordination entre les divers intervenants ;
5. apporter son concours aux services de l'État en matière de sécurité des systèmes d'information et des réseaux ;
6. effectuer un contrôle général de la sécurité des systèmes d'information et des réseaux relevant des divers organismes publics et privés identifiés par voie règlementaire ;
7. contrôler la conformité des signatures émises ;
8. centraliser les demandes d'assistance à la suite des incidents de sécurité sur les systèmes d'informations et les réseaux ;
9. assurer la veille technologique dans le domaine de la sécurité des systèmes d'information et des réseaux;
10. établir et maintenir une base de données des vulnérabilités ;
11. élaborer des recommandations sur la sécurité des systèmes d'information et des réseaux et veiller à leur mise en œuvre dans les organismes publics ;
12. diffuser des informations sur les précautions à prendre pour prévenir ou minimiser les risques d'incident ou leurs conséquences ;
13. collaborer avec l'Office National de Lutte contre la Cybercriminalité et toute autre entité publique dans le cadre de ses missions ;
14. participer aux activités de recherche, de formation et d'études afférentes à la sécurité des réseaux de communications électroniques, des systèmes d'information et de certification;

15. contribuer, en ce qui concerne ses missions, à l'application des accords, traités et conventions relatives à la lutte contre la cybercriminalité et la cybersécurité ratifiés par la République Démocratique du Congo ;
16. veiller à l'exécution des dispositions légales et règlementaires relatives à la sécurité des systèmes d'information et des réseaux ;
17. traiter toute question relative au développement des moyens ou prestations de cryptologie en République Démocratique du Congo ;
18. analyser les projets de textes législatifs et réglementaires en matière de cryptologie ;
19. analyser les normes techniques adoptées dans le domaine de la sécurité des systèmes d'information en général et celui de la cryptologie en particulier ;
20. recevoir les déclarations conformément à l'article 290 ;
21. octroyer des autorisations conformément à l'article 291 ;
22. étudier les demandes d'agréments des prestataires de services de cryptologie ;
23. demander et recevoir la communication des descriptions des caractéristiques techniques des moyens de cryptologie ;
24. prononcer des sanctions administratives à l'encontre des contrevenants aux dispositions du présent Chapitre ;
25. défendre les intérêts de la République Démocratique du Congo dans les instances et organismes régionaux et internationaux traitant de la cryptologie ;
26. mener des enquêtes et procéder aux contrôles des prestataires de services de cryptologie et de produits de cryptologie fournis ;
27. réceptionner les fichiers électroniques signés par des clés de cryptologie publiques ;
28. analyser et tester les logiciels, les équipements et les algorithmes de cryptologie ;
29. auditer les produits de cryptologie.

Article 288.

La composition, l'organisation et le fonctionnement de l'Agence sont fixées par l'ordonnance du Président de la République.

CHAPITRE II : DE L'OFFICE NATIONAL DE LUTTE CONTRE LA CYBERCRIMINALITE

Article 289.

Il est créé par décret du Premier Ministre, délibéré en conseil des Ministres, un organe de lutte contre la cybercriminalité, dénommé « Office National de lutte contre la Cybercriminalité », en sigle « ONLC ».

L'ONLC est un service public spécialisé placé sous l'autorité hiérarchique du Ministère ayant dans ses attributions la justice et dispose d'une compétence nationale.

Les agents de l'ONLC chargés des enquêtes ont la qualité d'officiers de police judiciaire.

Article 290.

L'ONLC a pour domaine de compétence, les infractions cybernétiques.

Article 291.

L'ONLC a pour missions notamment de :

1. de veiller à la prise de mesures préventives contre la cybercriminalité ;
2. d'animer et de coordonner, au niveau national, la mise en œuvre opérationnelle de la lutte contre les auteurs et complices d'infractions spécifiques à la criminalité liée aux technologies de l'information et de la communication ;
3. d'effectuer conformément au code de procédure pénale les enquêtes sur les infractions visant ou utilisant les systèmes informatiques ainsi que les modes de traitement, de stockage et de communication de l'information ;
4. d'apporter son concours technique aux autres services de sécurité à l'occasion des enquêtes en cours nécessitant ses compétences techniques ou son expertise ;
5. d'assurer en liaison avec les services compétents, les actions de formation et d'information visant à renforcer les capacités opérationnelles des agents de tous les services concourant à la lutte contre la cybercriminalité ;
6. d'intervenir, sous la direction de l'autorité judiciaire saisie, chaque fois que les circonstances l'exigent, pour s'informer sur place des faits relatifs aux investigations conduites.

Article 292.

La composition, l'organisation et le fonctionnement de l'ONLC sont fixés précisés par Décret du Premier Ministre délibéré en Conseil des Ministres.

Pour accomplir sa mission, l'ONLC centralise, analyse, exploite et communique aux services de la police nationale, de la direction générale des douanes et accises ainsi qu'aux autres

administrations et services publics de l'État concernés, toutes informations relatives aux faits et infractions liés aux technologies de l'information et de la communication en ce qui concerne leurs secteurs d'activités respectifs. Il établit également les liaisons utiles avec les organismes du secteur privé concernés.

Article 293.

Dans le cadre de la législation applicable, notamment en matière de secret professionnel, les services de la police nationale, de la direction générale des douanes et accises ainsi que les autres administrations et services publics de l'Etat concernés, adressent, dans les meilleurs délais, à l'ONLC les informations relatives aux infractions visées du présent Code dont ils ont connaissance.

Article 294.

Pour les infractions relevant de sa compétence définie au 1er alinéa de l'article 357, l'ONLC constitue, pour la République Démocratique du Congo, le point focal dans les échanges internationaux sur la cybercriminalité. Il contribue au niveau national à l'animation et à la coordination des travaux préparatoires nécessaires et participe aux activités des organes et enceintes institutions internationales sur la cybercriminalité.

Sans préjudice de l'application des conventions internationales, il entretient les liaisons opérationnelles avec les services spécialisés des autres pays et avec les organismes internationaux en vue de rechercher toute information relative aux infractions cybernétiques ainsi qu'à l'identification et à la localisation de leurs auteurs.

Article 295.

L'ONLC collabore avec toutes les administrations publiques ou privées qui sollicitent son assistance technique ou son expertise pour se mettre à l'abri des méfaits criminels liés aux technologies de l'information et de la communication.

L'Office National de lutte contre la Cybercriminalité collabore avec toutes les administrations publiques ou privées qui sollicitent son assistance technique ou son expertise pour prévenir les actes criminels liés aux technologies de l'information et de la communication.

TITRE IV : DE LA CYBERSECURITE

CHAPITRE 1 : DES OBLIGATIONS

Section 1 : DES OBLIGATIONS GÉNÉRALES

Article 296.

Toute personne, physique ou morale, opérant et/ou ayant des connaissances dans le secteur du numérique, est tenu de coopérer dans la détection des cyberattaques conformément aux dispositions légales et réglementaires applicables en République Démocratique du Congo.

Article 297.

Les fournisseurs des services en lignes sont tenus de détenir et de conserver les données de nature à permettre l'identification de quiconque aura contribué à la création du contenu ou de l'un des contenus des services dont ils sont prestataires.

Ils sont également tenus de fournir aux personnes qui éditent un service de communication au public en ligne des garanties permettant à celles-ci de satisfaire aux conditions d'identification prévues au présent Code.

L'Officier du Ministère Public ou l'Autorité de régulation peut requérir auprès des fournisseurs de services en ligne, conformément à la loi en la matière, la conservation et la protection de l'intégrité ainsi que la communication des données mentionnées au alinéa 1.

Article 298.

Les fournisseurs d'accès à internet et les fournisseurs de services en ligne ne sont pas responsables du contenu des informations qu'ils transmettent et auxquelles ils donnent accès, s'il satisfait aux conditions suivantes :

3. Ne pas être à l'origine de la transmission ;
4. Ne pas sélectionner le destinataire de la transmission ;
5. Ne pas modifier les informations faisant l'objet de la transmission ;
6. Informer leurs abonnés de l'existence des moyens techniques permettant de restreindre l'accès à certains services ou de les sélectionner et proposer au moins un de ces moyens.

Les fournisseurs d'accès à internet et les fournisseurs de services en ligne visées à l'alinéa 1er comprennent notamment le stockage automatique, intermédiaire et transitoire des informations transmises, pour autant que ce stockage serve exclusivement à l'exécution de la transmission sur le réseau de communication et que sa durée n'excède pas le temps raisonnablement nécessaire à la transmission.

Article 299.

Les fournisseurs d'accès à internet et les fournisseurs de services en ligne n'engagent pas leur responsabilité civile du fait des activités ou des informations stockées à la demande d'un destinataire de leurs 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 connaissance, ils ont agi promptement pour retirer ces données ou en rendre l'accès impossible.

L'alinéa précédent ne s'applique pas lorsque le destinataire du service agit sous l'autorité ou le contrôle du fournisseur de services en ligne.

Article 300.

Les fournisseurs d'accès à internet et les fournisseurs de services en ligne n'engagent pas leur responsabilité pénale, à raison des informations stockées à la demande d'un destinataire de leurs services, s'ils n'avaient pas effectivement connaissance de l'activité ou de l'information illicites ou si, dès le moment où ils en ont eu connaissance, ils ont agi promptement pour retirer ces informations ou en rendre l'accès impossible.

L'alinéa précédent ne s'applique pas lorsque le destinataire du service agit sous l'autorité ou le contrôle de la personne visée audit alinéa.

Article 301.

La connaissance des faits litigieux est présumée acquise par le fournisseur de services en ligne, lorsqu'il lui est notifié l'un des éléments suivants :

1. la date de la notification ;
2. si le notifiant est une personne physique : ses prénom, nom, postnom, profession, domicile, nationalité, date et lieu de naissance ;
3. si le notifiant est une personne morale : sa forme juridique, sa dénomination sociale et son siège ainsi que l'organe qui la représente légalement ;
4. le nom et domicile du destinataire ou, s'il s'agit d'une personne morale, sa dénomination sociale et son siège ;
5. la description des faits litigieux et, si possible, leur localisation précise ;
6. les motifs pour lesquels le contenu doit être retiré, comprenant la mention des dispositions légales et des justifications de faits ;
7. 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 302.

Les fournisseurs d'accès à internet et les fournisseurs de services en ligne ne sont pas soumis à l'obligation de surveiller les informations qu'ils transmettent ou stockent, ni à l'obligation de rechercher des faits ou des circonstances révélant des activités illicites sauf si, de manière

temporaire, cette obligation est faite à la demande de l'Officier du Ministère Public, l'Autorité de régulation, les services de sécurité et de maintien d'ordre public ou l'autorité judiciaire.

Article 303.

Les fournisseurs d'accès à internet et les fournisseurs de services en ligne doivent concourir à la lutte contre les infractions prévues dans le présent Code.

Ils doivent, à ce titre, mettre en place un dispositif facilement accessible et visible permettant à toute personne de porter à leur connaissance les faits constitutifs de ces infractions.

Ils sont également tenus, d'une part, d'informer promptement les autorités compétentes de toutes activités illicites mentionnées qui leur seraient signalées et qu'exerceraient les destinataires de leurs services, et, d'autre part, de rendre publics les moyens qu'elles consacrent à la lutte contre ces activités illicites.

L'autorité judiciaire peut enjoindre, conformément à la loi, à tout fournisseur de services en ligne, et à défaut, à tout fournisseur d'accès à Internet, toutes mesures propres à prévenir un dommage ou à faire cesser un dommage occasionné par le contenu d'un service en ligne.

Article 304.

Les personnes dont l'activité est d'éditer un service de communications au public en ligne, sont tenues de mettre à la disposition de leurs abonnés, dans un standard ouvert, les éléments suivants :

1. pour les personnes physiques : leurs prénom, nom, postnom, domicile et numéro de téléphone ;
2. pour les personnes morales : leurs forme sociale, dénomination sociale, numéro de téléphone, numéro du Registre du Commerce et du Crédit Mobilier, numéro d'identification nationale, capital social ainsi que le siège social ;
3. le nom du directeur et du codirecteur de la publication et, le cas échéant, celui du responsable de la rédaction ;
4. le nom, la dénomination sociale, l'adresse ainsi que le numéro de téléphone du fournisseur de services en ligne.

Article 305.

Les personnes éditant à titre non professionnel un service de communications au public en ligne peuvent ne tenir à la disposition du public, pour préserver leur anonymat, que le nom, la dénomination sociale et l'adresse du fournisseur de services en ligne, sous réserve de lui avoir communiqué les éléments d'identification prévus au présent article.

Les fournisseurs d'accès à internet et les fournisseurs de services en ligne sont tenus à une obligation de confidentialité pour tout ce qui concerne la divulgation de ces éléments d'identification ou de toute information permettant d'identifier la personne concernée.

Cette obligation de confidentialité n'est pas opposable à l'autorité judiciaire, ni aux services d'enquête de la police judiciaire, ni à l'Autorité de régulation, l'Autorité de protection des données, ainsi que les services de sécurité lorsqu'ils requièrent pour les besoins d'ordre public.

SECTION 2 : DES OBLIGATIONS SPÉCIFIQUES

Article 306.

Les fournisseurs de cache ne sont pas responsables des données et informations qu'ils traitent dans le cadre de leurs activités, s'ils réunissent les conditions suivantes :

1. ne pas modifier l'information ;
2. se conformer aux conditions d'accès à l'information ;
3. se conformer aux règles concernant la mise à jour de l'information, indiquées d'une manière largement reconnue et utilisée dans le secteur ;
5. ne pas entraver l'utilisation légale de la technologie, largement reconnue et utilisée par le secteur, dans le but d'obtenir des données sur l'utilisation de l'information ;
6. agir promptement pour retirer l'information stockée ou pour rendre l'accès à celle-ci impossible dès qu'ils ont 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'une autorité administrative ou judiciaire a ordonné de retirer l'information ou de rendre l'accès à cette dernière impossible.

Article 307.

Les fournisseurs de liens hypertextes ne sont pas responsables des informations auxquelles ils donnent accès, dès lors que :

1. ils suppriment ou empêchent rapidement l'accès aux informations après avoir reçu une injonction de l'autorité judiciaire de retirer le lien hypertexte ;
2. ayant pris connaissance ou conscience d'informations illégales spécifiques stockées ou des activités illégales qu'exerceraient les destinataires de leurs services, autrement que par une injonction de l'autorité judiciaire, ils informent rapidement les autorités judiciaires pour leur permettre d'évaluer la nature des informations ou des activités et, si nécessaire, d'ordonner le retrait du contenu.

Article 308.

Les fournisseurs de moteurs de recherche qui, de manière automatique ou sur la base des entrées effectuées par autrui, créent un index des contenus en ligne ou mettent à disposition des moyens électroniques pour rechercher les informations fournies par des tiers, ne sont pas responsables des résultats de recherche, à condition qu'ils :

1. ne soient pas à l'origine de la transmission ;

2. ne sélectionnent pas le destinataire de la transmission ;
3. ne sélectionnent pas ou ne modifient pas les informations contenues dans la transmission.

Article 309.

L'hébergeur n'est pas responsable des informations stockées à la demande d'un utilisateur du service qu'il fournit, à condition que :

1. lorsqu'il a connaissance d'informations illégales, spécifiques, stockées ou des activités illégales qu'exerceraient les destinataires du service, il en informe immédiatement l'autorité judiciaire.
2. l'hébergeur retire, rend l'accès impossible ou désactive promptement l'accès aux données après avoir reçu de l'autorité judiciaire une injonction de retirer les données.

L'alinéa 1 du présent article ne s'applique pas lorsque le destinataire du service agit sous l'autorité ou le contrôle de l'hébergeur.

Article 310.

Les vendeurs de produits et/ou fournisseurs de services des technologies de l'information et de la communication sont tenus de solliciter, auprès du Ministre ayant le numérique dans ses attributions, un certificat de conformité après analyse de vulnérabilité et évaluation de la garantie de sécurité par les experts en sécurité informatique agréés par ledit Ministre.

Ils sont, en outre, tenus d'informer les consommateurs de toutes les vulnérabilités décelées dans les produits et services des technologies de l'information et la communication ainsi que des solutions déployées pour y remédier.

Article 311.

Les fournisseurs 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 services exploitant ces systèmes sont délivrés par le Ministère ayant le numérique dans ses attributions.

Article 312.

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.

Ces contrôles sont effectués par l'Agence Nationale de Sécurité des Systèmes d'Information « ANSSI en sigle ».

Le coût des contrôles est à la charge de l'opérateur.

Article 313.

Pour les besoins de la sécurité des systèmes d'information et des opérateurs, l'ANSSI peut obtenir des opérateurs, 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.

CHAPITRE II : DE LA CRYPTOLOGIE

SECTION I : DES DISPOSITIONS GENERALES

Article 314.

L'utilisation, la fourniture, l'importation et l'exportation des moyens de cryptologie assurant exclusivement des fonctions d'authentification ou de contrôle d'intégrité sont libres, sous réserve des obligations prévues dans le présent Livre.

Néanmoins, lorsque les moyens de cryptologie permettent d'assurer des fonctions de confidentialité, le principe de libre utilisation visé à l'alinéa 1 s'applique uniquement si les moyens s'appuient sur des conventions gérées par un prestataire agréé.

Les prestations de services de cryptologie sont réservées aux prestataires de services de cryptologie, selon les modalités déterminées en vertu du présent chapitre, sauf dans le cas où le cryptage est fait pour ses propres données.

Article 315.

Nul ne peut opérer une activité de cryptologie sans se soumettre à l'un des régimes juridiques prévus dans le présent Livre.

SECTION II : DES REGIMES JURIDIQUES

Article 316.

L'exercice des activités et services de cryptologie est soumis au régime d'autorisation ou de déclaration, conformément aux modalités et conditions d'octroi fixées dans le Livre 1 du présent Code et par arrêté du Ministre ayant le numérique dans ses attributions.

L'instruction des demandes d'autorisation ou de déclaration, ainsi que l'élaboration du cahier de charges relève de la Commission cryptologie.

Article 317.

La fourniture ou l'importation de moyens de cryptologie n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité est soumise à une déclaration préalable

auprès de la Commission cryptologie, sous réserve des éventuelles dispenses de déclaration en vertu d'une disposition légale ou réglementaire.

Article 318.

Le prestataire ou la personne procédant à la fourniture, à l'importation ou à l'exportation d'un moyen de cryptologie tient à la disposition de la Commission cryptologie une description des caractéristiques techniques des moyens de cryptologie utilisés.

Article 319.

L'exportation de moyens de cryptologie n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité est soumise à l'autorisation du Ministre ayant le numérique dans ses attributions, la Commission cryptologie entendue.

SECTION III : DES PRESTATAIRES DE SERVICES DE CRYPTOLOGIE

Article 320.

Les prestataires de services de cryptologie sont tenus d'obtenir une autorisation préalable auprès de la Commission cryptologie.

Les conditions de délivrance de l'agrément aux prestataires de services de cryptologie ainsi que leurs obligations sont définies par arrêté du Ministre ayant le numérique dans ses attributions.

Article 321.

La Commission cryptologie peut, sur instruction du Ministre ayant le numérique dans ses attributions, prévoir des exceptions à cette obligation d'autorisation préalable pour les prestations des services de cryptologie dont les caractéristiques techniques ou les conditions de fourniture sont telles que, au regard des intérêts de la défense nationale et de la sécurité intérieure ou extérieure de l'Etat, cette fourniture peut être dispensée de toute formalité préalable.

Article 322.

Le prestataire de services de cryptologie est entièrement responsable du préjudice causé aux personnes :

1) 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;
2) qui se sont fiées raisonnablement au service de cryptologie fourni. Toute clause contractuelle contraire est réputée non écrite.

Le prestataire de services de cryptologie peut toutefois dégager ou limiter sa responsabilité s'il parvient à démontrer l'absence de négligence ou de faute intentionnelle.

Les prestataires de services de cryptologie sont exonérés de toute responsabilité à l'égard des personnes qui font un usage non autorisé de leurs services, pour autant que les conditions d'utilisation soient aisément accessibles aux utilisateurs et précisent clairement les usages autorisés et non autorisés.

Les prestataires de services de cryptologie doivent obligatoirement contracter une police d'assurance couvrant les risques liés à l'exercice de leurs activités.

SECTION IV : DES SANCTIONS ADMINISTRATIVES

Article 323.

Lorsqu'un prestataire de services de cryptologie, même à titre gratuit, ne respecte pas les obligations auxquelles il est assujetti en application du présent Livre, la Commission cryptologie peut, après audition de l'intéressé, prononcer :

1) l'interdiction d'utiliser ou de mettre en circulation le moyen de cryptologie concerné. Ce moyen pourra être remis en circulation dès que les obligations antérieurement non respectées auront été satisfaites, dans les conditions prévues dans les dispositions du présent Chapitre ;
2) le retrait provisoire de l'autorisation accordée pour une durée comprise entre un et douze mois ;
3) le retrait définitif de l'autorisation accordée ;
4) le paiement des amendes dont le montant est fixé en fonction de la gravité des manquements commis et en relation avec les avantages ou les profits tirés de ces manquements

L'interdiction de mise en circulation prévue à l'alinéa 1er point 1 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, 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 des diffuseurs commerciaux.

Le moyen de cryptologie concerné peut être remis en circulation dès que les obligations antérieurement non respectées auront été satisfaites.

TITRE III : DE LA LUTTE CONTRE LA CYBERCRIMINALITE

CHAPITRE 1 : DES PRINCIPES GENERAUX

SECTION 1 : DE LA RESPONSABILITE PENALE

Article 324.

L'Etat, les provinces, les entités territoriales décentralisées, les autorités administratives indépendantes et les établissements publics n'engagent pas leurs responsabilités pénales.

Les agents de l'État ou fonctionnaires publics œuvrant pour l'État, les provinces, les entités territoriales décentralisées, les autorités administratives indépendantes et les établissements publics engagent leur responsabilité pénale individuelle lorsqu'elles commettent des infractions dans les mêmes circonstances et dans l'exercice de leurs fonctions.

Toutefois, la responsabilité des personnes morales n'exclut pas celle des personnes physiques auteurs ou complices des mêmes faits, agissant à titre individuel.

Article 325.

Les personnes morales de droit privé sont responsables des infractions prévues par les dispositions du Présent Code lorsqu'elles sont commises pour leur compte par l'un de leurs représentants.

Les dirigeants des personnes morales de droit privé engagent leur responsabilité pénale individuelle lorsqu'elles commettent des infractions dans les mêmes circonstances et dans l'exercice de leurs fonctions.

SECTION 2 : DES PEINES

Article 326.

Les peines applicables en matière d'infractions relatives à la cybercriminalité sont :

1. La servitude pénale ;
2. L'amende ;
3. La confiscation spéciale.

Article 327.

Les peines encourues par les personnes morales, pour les infractions visées au présent Code, sont les suivantes :

1. une amende dont le montant maximum est égale 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 ou, lorsqu'il s'agit d'une infraction qui porte atteinte à la sécurité et sureté de l'Etat ;
3. l'interdiction définitive ou pour une durée de deux à cinq ans d'exercer directement ou indirectement une ou plusieurs activités professionnelles ou sociales ;
4. la fermeture définitive ou pour une durée de deux à cinq ans d'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ;
5. l'exclusion définitive des marchés publics ou pour une durée de deux à cinq ans ;
6. l'interdiction définitive ou pour une durée de deux à cinq ans de faire appel public à l'épargne ;
7. l'interdiction pour une durée de deux à cinq ans d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés ou d'utiliser des cartes de paiement ;
8. la confiscation de l'outil qui a servi à commettre l'infraction et du produit de l'infraction.

Article 328.

Sans préjudice des dispositions du Code pénal congolais, en cas de condamnation à l'une des infractions prévues au présent Livre, la juridiction compétente peut prononcer la confiscation des matériels, des équipements, des instruments, des systèmes informatiques ou des données informatiques ainsi que des biens numéraires, avantages ou produits résultant de l'infraction.

Les décisions de condamnation prises en vertu de l'alinéa précédent sont publiées dans le Journal officiel de la République Démocratique du Congo.

Article 329.

Sans préjudice des dispositions du Code pénal congolais, en cas de condamnation pour l'une des infractions prévues au présent code, la juridiction compétente prononce l'interdiction selon les modalités prévues au présent article.

Cette peine comprend l'interdiction d'émettre des messages de communications électroniques et l'interdiction à titre provisoire ou définitif de l'accès au site ayant servi à commettre l'infraction voire à tout autre site quel qu'il soit, pour une durée d'un an à dix ans.

La juridiction compétente peut faire injonction à toute personne responsable légalement du site ayant servi à commettre l'infraction et/ou à toute autre 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 juridiction compétente peut prononcer à l'encontre du condamné pour les infractions prévues par le présent Livre, l'interdiction à titre définitif ou pour une durée de cinq ans à dix ans, d'exercer toute activité en relation avec le secteur des communications électroniques ou d'exercer une fonction publique, un mandat électif ou une fonction dans une entreprise dont l'Etat est totalement ou partiellement propriétaire ou une activité socio-professionnelle, lorsque les faits ont été commis dans l'exercice ou à l'occasion de l'exercice des fonctions.

La juridiction compétente peut interdire en tout ou partie l'exercice des droits civiques et civils suivants :

- droit de vote;
- droit d'éligibilité ;
- interdiction d'accès aux fonctions publiques et paraétatique quel qu'en soit l'échelon.
- droit d'être expert ou témoins dans les actes d'état civil ;
- droit de déposer en justice, autrement que pour y donner de simples renseignements.

La violation des interdictions prononcées par les tribunaux est punie d'une peine de servitude pénale de six mois à trois ans et d'une amende de trois cent mille à cinq millions de francs Congolais.

Les décisions de condamnation prises en vertu du présent article sont publiées dans le Journal officiel de la République Démocratique du Congo.

SECTION 3 : DE LA PARTICIPATION CRIMINELLE ET DE LA TENTATIVE PUNISSABLE

Article 330.

Est puni de la même peine que l'infraction consommée, toute participation criminelle et toute tentative de violation du présent Code.

SECTION 4 : DE LA RECIDIVE ET DES CIRCONSTANCES AGGRAVANTES

Article 331.

Lorsqu'une des infractions prévues par le présent Livre est commise dans les cinq ans qui suivent le prononcé de la condamnation devenue irrévocable pour l'une de ces infractions, la peine prévue par la loi est doublée.

Article 332.

Lorsqu'une infraction est commise par un membre d'une organisation criminelle ou d'une bande organisée en vue de commettre des infractions punies par le présent Livre, la peine initialement prévue est doublée.

Lorsque l'une des infractions prévues en vertu du présent Livre porte atteinte à la sureté de l'Etat, des données informatiques ou aux systèmes informatiques liés à des infrastructures et applications stratégiques ou sensibles, le juge prononce la peine de servitude pénale à perpétuité et une amende d'un milliard de francs Congolais.

CHAPITRE II : DES REGLES DE PROCEDURE ET DE COMPETENCE DES JURIDICTIONS

SECTION 1 : DE LA CONSTATATION DES INFRACTIONS A LA LESGISLATION DU NUMERIQUE

Article 333.

Les Agents de l'Administration près le Ministère ayant le numérique dans ses attributions et ceux des autorités de régulation, ayant au moins le grade d'attaché de bureau de première classe sont revêtus de la qualité d'officiers de police judiciaire à compétence restreinte et ont le pouvoir de constater les infractions à la législation du numérique.

Lorsque les officiers de police judiciaire à compétence générale constatent des infractions à la législation du numérique, ils les signalent aux agents de l'Administration près le Ministère ayant le numérique dans ses attributions et ceux de des autorités de régulation ayant la qualité d'officiers de police judiciaire à compétence restreinte.

Article 334.

Les infractions à la législation du numérique doivent être constatées dans des procès-verbaux établis conformément au Code de procédure pénale.

SECTION 2 : DE LA PERQUISITION DES DONNÉES STOCKÉES DANS UN SYSTÈME INFORMATIQUE

Article 335.

Lorsque des données stockées dans un système informatique ou sur un support permettant de conserver des données sur le territoire congolais, sont utiles à la manifestation de la vérité, l'officier du Ministère Public, conformément aux dispositions prévues aux articles 22 et 23 du Code de procédure pénale, peut opérer une perquisition ou accéder à un système informatique ou à une partie de celui-ci ou dans un autre système informatique ou un support et aux données présentes dans ces derniers dès 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 l'Officier du Ministère Public, par voie de commission rogatoire internationale.

Article 336.

Lorsque l'Officier du Ministère Public 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, elles peuvent être de plus rendues inaccessibles ou retirées du système informatique en question sous ordre du juge.

SECTION 3 : DE L'INTERCEPTION DES DONNÉES

Article 337.

L'Officier du Ministère public peut, lorsque les nécessités de l'information l'exigent, prescrire l'interception, l'enregistrement et la transcription de correspondances conformément aux dispositions du présent Code, y compris des données relatives au contenu, émises par voie de communications électroniques.

Article 338.

L'Autorité de régulation peut autoriser :

1) les interceptions de correspondances émises par la voie des communications électroniques, conformément aux dispositions du présent Code ;
2) la conservation et la protection de l'intégrité ainsi que le recueil, y compris en temps réel suivant les modalités prévues aux articles 25 et suivants du Code de procédure pénale, des données et renseignements sur les données personnelles et à l'article 265 du présent Code.

Les modalités de mise en œuvre des dispositions du présent article seront précisées par voie règlementaire.

Article 339.

Les opérations d'interception visées par le présent Code peuvent être autorisées lorsqu'elles sont nécessaires :

1) au maintien de l'indépendance nationale, de l'intégrité du territoire ou de la défense nationale ;
2) à la préservation des intérêts majeurs de la politique étrangère de la République Démocratique du Congo ;
3) à la sauvegarde des intérêts économiques, industriels et scientifiques majeurs de la République Démocratique du Congo ;
4) à la prévention du terrorisme, des violences collectives de nature à porter gravement atteinte à l'ordre public ou de la criminalité et de la délinquance organisées.

SECTION 4 : DES POURSUITES

Article 340.

Les infractions à la législation du numérique sont poursuivies et prouvées par toute voie de droit.

Article 341.

L'action publique contre les infractions à la législation du numérique est exercée conformément au Code de procédure pénale.

L'action pour l'application des amendes prévues pour les infractions à la législation du numérique est exercée par les officiers de police judiciaires à compétence restreinte au sens du présent Code.

SECTION 5 : DE L'EXTINCTION DE L'ACTION PUBLIQUE

Article 342.

L'amende transactionnelle prononcée par les officiers de police judiciaire à compétence restreinte au sens du présent Code éteint définitivement l'action pour l'application des amendes et confiscation, ainsi que l'action pour l'application des peines de servitude pénale, lorsqu'elle intervient avant toute saisine du tribunal compétent.

Article 343.

L'action publique en répression des infractions à la législation du numérique se prescrit par les délais ci-dessous arrêtés :

1. trois ans, si l'infraction n'est punie que d'une peine d'amende ou si le maximum de la servitude pénale applicable ne dépasse pas trois ans;
2. dix ans, si l'infraction est punie de plus de trois ans de servitude pénale.

Ces délais de prescription commencent à courir du jour de la commission du fait infractionnel ou, s'il a été dissimulé, du jour de sa découverte ou de sa révélation.

Article 344.

La prescription sera interrompue, selon le cas, par des actes d'instruction ou de poursuite, portés à la connaissance de l'auteur, dans les délais de trois ou dix ans, à compter du jour où l'infraction est commise ou du jour où elle a été découverte.

SECTION 6 : DES JURIDICTIONS COMPETENTES

Article 345.

Les règles de compétence et de procédure applicables en matière d'infractions à la législation du numérique sont celles prévues respectivement par la loi organique n°13/011-B du 11 avril 2013 portant organisation, fonctionnement et compétence des juridictions de l'ordre judiciaire et le Code de procédure pénale.

Toutefois, le tribunal de commerce est compétent pour toutes les infractions prévues par le présent Code qui portent atteinte à la législation économique et commerciale quel que soit le taux de la servitude pénale ou la hauteur de l'amende.

Article 346.

Sans préjudice du code pénal, les juridictions visées à l'article précédent sont compétentes lorsque :

1) l'infraction a été commise sur Internet sur le territoire de la République Démocratique du Congo dès lors que le contenu illicite est accessible depuis la République Démocratique du Congo ;
2) la personne physique ou morale s'est rendue coupable, sur le territoire de la République Démocratique du Congo, comme complice d'une infraction commise à l'étranger si l'infraction est punie à la fois par la loi congolaise et par la loi étrangère ;
3) l'infraction a été commise par des Congolais hors du territoire de la République Démocratique du Congo et que les faits sont punis par la législation du pays où ils ont été commis.

CHAPITRE III : DE LA QUALIFICATION DES INFRACTIONS

SECTION PRELIMINAIRE :

Article 347.

Constitue une infraction à la législation du numérique, toute violation de celle-ci qui est passible d'une peine prévue par le présent Code ou par les dispositions légales ou règlementaires édictées pour son application.

Hormis les dispositions de l'alinéa 1 du présent article, le présent Code définit et réprime des infractions spécifiques liées aux technologies de l'information et de la communication.

SECTION 1 : DES INFRACTIONS DE DROIT COMMUN COMMISES AU MOYEN D'UN OU SUR UN RESEAU DE COMMUNICATION ELECTRONIQUE OU UN SYSTÈME INFORMATIQUE

Article 348.

Les infractions de droit commun commises au moyen d'un ou sur un réseau de communication électronique ou un système informatique sont réprimées conformément au Code pénal congolais et aux dispositions particulières en vigueur.

SECTION 2 : DES ATTEINTES AUX RESEAUX ET SYSTEMES D'INFORMATION

Paragraphe 1 : De l'accès et du maintien illégal

Article 349.

Quiconque accède ou se maintient intentionnellement et sans droit, dans l'ensemble ou partie d'un système informatique est puni d'une peine de servitude pénale d'un an à cinq ans et d'une amende de cinq cent mille à un million de francs Congolais ou de l'une de ces peines seulement.

Article 350.

Quiconque accède ou se maintient intentionnellement et sans droit, dans l'ensemble ou partie d'un système informatique, avec une intention frauduleuse est puni d'une peine de servitude pénale de deux à cinq ans et d'une amende de cinq cent mille à deux millions de francs Congolais ou de l'une de ces peines seulement.

Article 351.

Quiconque, avec une intention frauduleuse ou dans le but de nuire, outrepasse son pouvoir d'accès légal à un système informatique, est puni d'une peine de servitude pénale de deux à cinq ans et d'une amende de cinq cent mille à deux millions de francs congolais ou de l'une de ces peines seulement.

Article 352.

Lorsqu'il résulte des faits visés **aux articles 297 à 299** du présent Code soit la suppression, l'obtention ou la modification de données contenues dans le système informatique, soit une altération du fonctionnement de ce système informatique, les peines prévues par ces dispositions sont doublées.

Lorsque les faits visés aux articles **297 à 299** du présent Code sont commis en violation de mesures de sécurité, l'auteur de ces faits est puni de peine de servitude pénale de dix à vingt ans et une amende de cinq millions francs Congolais à cinq cent millions de francs congolais.

L'accès suivant les mesures de sécurité, pour une durée déterminée, à des systèmes informatiques est autorisé sans que le secret professionnel ou bancaire puisse être opposé conformément aux dispositions du Code de procédure pénale.

Paragraphe 2 : Des atteintes aux données

Article 353.

Est puni d'une servitude pénale de deux à cinq ans et d'une amende de cinq cent mille à deux millions de francs Congolais, celui qui intercepte, divulgue, utilise, altère ou détourne intentionnellement et sans droit par des moyens techniques, des données lors de leur transmission non publique à destination, en provenance ou à l'intérieur d'un système informatique, y compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données.

Article 354.

Est puni d'une servitude pénale de cinq à dix ans et d'une amende de cinq millions à cent millions de francs congolais, celui qui transfère sans autorisation des données d'un système informatique ou d'un moyen de stockage de données informatique.

La peine prévue à l'alinéa précédent pourra être porté au double du maximum, cette infraction est commise avec une intention frauduleuse, ou en rapport avec un système informatique connecté à un autre système informatique, ou en contournant les mesures de protection mises en place pour empêcher l'accès au contenu de la transmission non publique

Toutefois, une personne ne commet pas d'infraction au sens du présent article si :

1) l'interception est réalisée conformément à un mandat de justice ;
2) la communication est envoyée par ou est destinée à une personne qui a consenti à l'interception ;
3) une personne morale est légalement autorisée pour les besoins de la sécurité publique ou de la défense nationale ;
4) une personne morale ou physique est légalement autorisée en vertu des dispositions légales et règlementaires en vigueur en République Démocratique du Congo.

Paragraphe 3 : Des atteintes à l'intégrité du système

Article 355.

Est puni d'une peine de servitude pénale de deux à cinq ans et d'une amende de cinq millions à cinq cents millions de francs Congolais ou de l'une de ces peines seulement, celui qui, intentionnellement et sans droit, directement ou indirectement, provoque par tout moyen technologique une interruption du fonctionnement normal d'un système informatique.

Quiconque, suite à la commission des faits visés à l'alinéa 1, aura causé un dommage à des données dans le système informatique concerné ou dans tout autre système informatique, sera puni d'une peine de servitude pénale de cinq à dix ans et d'une amende de cinq millions à cinq cents millions de francs Congolais ou de l'une de ces peines seulement.

Quiconque, suite à la commission des faits visés à l'alinéa 1, aura provoqué une perturbation grave ou empêche, totalement ou partiellement, le fonctionnement normal du système informatique concerné ou de tout autre système informatique, sera condamné à la peine de servitude pénale de dix à vingt ans et à une amende de cinq millions à cinq cents millions de francs Congolais ou de l'une de ces peines seulement.

Lorsque la commission des faits visés à l'alinéa 1 touche une ou plusieurs infrastructures sensibles ou critiques, au sens du présent Code, la personne responsable est condamnée à la peine de servitude pénale de dix à vingt ans et à une amende de cinq millions à cinq cents millions de francs Congolais ou de l'une de ces peines seulement.

Lorsque la commission des faits visés à l'alinéa 1 touche une ou plusieurs infrastructures sensibles ou critiques, au sens du présent Code, la personne responsable est condamnée à la peine de servitude pénale de dix à vingt ans et à une amende de cinq millions à cinq cents millions de francs Congolais ou de l'une de ces peines seulement.

La peine de servitude pénale et l'amende sont applicables même si les conséquences sur le ou les systèmes informatiques visés aux alinéas précédents sont temporaires ou permanentes.

Paragraphe 4 : Des atteintes à l'intégrité des données

Article 356.

Celui qui, intentionnellement et sans droit, directement ou indirectement endommage, efface, détériore, altère ou supprime des données, sera puni d'une peine de servitude pénale de six mois à cinq ans et d'une amende de cinq cents mille à deux millions de francs Congolais ou de l'une de ces peines seulement.

Si l'infraction visée à l'alinéa 1 est commise avec une intention frauduleuse ou dans le but de nuire, la peine de servitude pénale est de deux à cinq ans et d'une amende de cinq cents mille francs à deux millions de francs Congolais ou l'une de ces peines seulement.

Paragraphe 5 : Des abus de dispositifs

Article 357.

Quiconque aura, intentionnellement et sans droit, produit, vendu, obtenu en vue de son utilisation, importé, exporté, diffusé ou mis à disposition sous une autre forme, un quelconque dispositif, y compris des données ou des programmes informatiques, principalement conçu ou adapté pour permettre la commission d'une ou plusieurs infractions prévues dans le présent

Code, sera puni d'une peine de servitude pénale de deux à cinq ans et d'une amende de cinq cents mille à deux millions de francs Congolais ou de l'une de ces peines seulement.

Quiconque, intentionnellement et sans droit, aura possédé au sens du présent Code, dans l'intention de l'utiliser, un quelconque dispositif, y compris des données, principalement conçu ou adapté pour permettre la commission d'une ou plusieurs infractions visées au Titre I du présent Livre est puni d'une peine de servitude pénale de six mois à cinq ans et d'une amende de cinq cents mille à deux millions de francs Congolais ou de l'une de ces peines seulement.

Est puni d'une peine de servitude pénale de deux à cinq ans et d'une amende de cinq cents mille à deux millions de francs Congolais ou de l'une de ces peines seulement, tout officier ou fonctionnaire public, dépositaire ou agent de la force publique qui, à l'occasion de l'exercice de ses fonctions, hors les cas prévus par la loi ou sans respecter les formalités qu'elle prescrit, indûment, possède, produit, vend, obtient en vue de son utilisation, importe, diffuse ou met à disposition sous une autre forme un dispositif, y compris des données, principalement conçu ou adapté pour permettre la commission d'une ou plusieurs infractions visées dans le présent Code.

Paragraphe 6 : De la falsification des données

Article 358.

Est puni d'une peine de servitude pénale de cinq à dix ans et d'une amende de cinq millions à cinquante millions de Francs congolais ou de l'une de ces peines seulement, quiconque commet un faux, en introduisant, intentionnellement et sans droit, dans un système informatique, en modifiant, altérant ou effaçant des données, qui sont stockées, traitées ou transmises par un système informatique, ou en modifiant par tout moyen technologique l'utilisation possible des données dans un système informatique, et ce dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si les données falsifiées étaient authentiques.

Quiconque cherchant à se procurer, pour lui-même ou pour autrui, avec une intention frauduleuse, un avantage économique en introduisant dans un système informatique, en modifiant ou effaçant des données qui sont stockées, traitées ou transmises par un système informatique, ou en modifiant par tout moyen technologique l'utilisation normale des données dans un système informatique, sera puni d'une peine de servitude pénale de cinq à dix ans et d'une amende de cinq millions à cinquante millions de Francs congolais ou de l'une de ces peines seulement.

Quiconque aura, en connaissance de cause, décide de faire usage de données falsifiées, au sens des alinéas 1 et 2, sans en être l'auteur, sera puni d'une peine de servitude pénale de cinq à dix ans et d'une amende de cinq millions à cinquante millions de Francs congolais ou de l'une de ces peines seulement, comme s'il était l'auteur de la falsification des données.

Paragraphe 7 : De la fraude informatique

Article 359.

Quiconque aura, intentionnellement et sans droit, causé ou cherché à causer un préjudice à autrui avec l'intention de procurer un avantage économique illégal à soi-même ou à un tiers, sera puni d'une peine de servitude pénale de cinq à dix ans et d'une amende de cinq millions à cinquante millions de Francs congolais :

1) S'il a introduit dans un système informatique, en modifiant, altérant ou effaçant des données qui sont stockées, traitées ou transmises par un système informatique ;
2) S'il perturbe le fonctionnement normal d'un système informatique ou des données y contenues.

SECTION 3 : DES ATTEINTES DANS LE DOMAINE DE LA CRYPTOLOGIE

Article 360.

Est puni d'une amende de cinq à dix millions de Francs congolais, quiconque n'aura pas satisfait à l'obligation de communication à la Commission Cryptologie d'une description des caractéristiques techniques du moyen de cryptologie dans les conditions prévues par les dispositions du Titre II du présent Livre et de ses textes d'application.

Article 361.

Est puni d'une amende de cinq à dix millions de Francs congolais, quiconque fournit ou importe un moyen de cryptologie n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité sans satisfaire à l'obligation de déclaration préalable auprès de la Commission cryptologie, sans préjudice de l'application du code des douanes.

Est puni de cinq à dix ans de servitude pénale et d'une amende de cinq à dix millions de francs Congolais, quiconque aura fourni des prestations de cryptologie sans avoir obtenu préalablement l'agrément de la Commission cryptologie.

Article 362.

Est puni de cinq à dix ans de servitude pénale et d'une amende de cinq à dix millions de Francs congolais, ou de l'une de ces peines seulement, quiconque aura exporté un moyen de cryptologie n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité sans avoir obtenu préalablement l'autorisation de la Commission cryptologie, sans préjudice de l'application du Code des douanes.

Article 363.

Est puni de cinq à dix ans de servitude pénale et d'une amende de cinq à dix millions de Francs congolais, ou de l'une de ces peines seulement, quiconque aura mis à la disposition d'autrui par la vente ou la location un moyen de cryptologie ayant fait l'objet d'une interdiction administrative d'utilisation et de mise en circulation, sans préjudice de l'application du Code des douanes.

Article 364.

Est puni de cinq à dix ans de servitude pénale et d'une amende de cinq à dix millions de Francs congolais, ou de l'une de ces peines seulement, quiconque aura fait obstacle au déroulement des enquêtes au sens du Code de procédure pénale et du présent Code ou refusé de fournir des informations ou documents y afférents, sans préjudice de l'application du code des douanes.

Article 365.

Lorsqu'un moyen de cryptologie a été utilisé pour préparer ou commettre une infraction ou pour en faciliter la préparation ou la commission, le maximum de la peine prévu par le Code pénal est porté au double, hormis la servitude pénale à perpétuité.

Les dispositions de l'alinéa 1 ne sont pas applicables à l'auteur ou au complice de l'infraction qui, à la demande des autorités compétentes, leur a remis la version intelligible des messages chiffrés, ainsi que les conventions secrètes nécessaires au déchiffrement.

Article 366.

Est puni de trois ans de servitude pénale et d'une amende d'un million à vingt millions de Francs congolais, quiconque ayant connaissance de la convention secrète de déchiffrement d'un moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre une infraction, refuse de remettre ladite convention aux autorités judiciaires ou de la mettre en œuvre, sur les réquisitions de ces autorités délivrées en application du Code de procédure pénale.

Si le refus est opposé alors que la remise ou la mise en œuvre de la convention permet d'éviter la commission d'une infraction ou d'en limiter les effets, la peine est portée à cinq ans de servitude pénale et d'une amende de cinq millions à vingt millions de francs congolais.

SECTION 4 : DES INFRACTIONS LIEES A L'UTILISATION DES DONNEES A CARACTERE PERSONNEL

Paragraphe 1 : De l'envoi de messages non sollicités

Article 367.

Tout message électronique non sollicité envoyé sur base de la collecte de données à caractère personnel doit contenir un lien pouvant permettre au bénéficiaire de se désabonner.

Le non-respect de cette disposition expose le contrevenant à une amende de cinq cent mille à deux millions de francs congolais.

Paragraphe 2 : De la tromperie

Article 368.

Est puni d'une peine de servitude pénale de six mois à deux ans et d'une amende de vingt-cinq millions de Francs congolais, ou d'une de ces peines seulement, celui qui 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.

Paragraphe 3 : Du détournement des fonds

Article 369.

Quiconque aura utilisé 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 servitude pénale de cinq à dix ans et d'une amende de vingt millions à cent millions de francs Congolais.

Paragraphe 4 : Du traitement non autorisé

Article 370.

Quiconque aura procédé à un traitement de données à caractère personnel soit sans avoir préalablement informé individuellement les personnes concernées 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 sera puni d'une peine de servitude pénale de six mois à deux ans et d'une amende de deux millions à cinq millions de Francs congolais, ou l'une de ces peines seulement.

Paragraphe 5 : De l'usurpation d'identité

Article 371.

Est puni d'une servitude pénale de six mois à cinq ans et d'une amende de vingt millions à cent millions de Francs congolais, quiconque usurpe, intentionnellement et sans droit par le biais d'un système informatique, l'identité d'autrui ou une ou plusieurs données permettant de s'attribuer faussement l'identité d'autrui à dessein de troubler sa tranquillité, de porter atteinte à son honneur, à sa considération ou à ses intérêts.

Quiconque, en se prévalant intentionnellement à tort d'un motif ou d'une justification légitime et en utilisant un système informatique à toute étape de l'infraction, aura transféré, possédé ou utilisé un moyen de s'identifier à une autre personne dans l'intention de commettre, d'aider ou d'encourager une activité illégale, est puni d'une servitude pénale d'un à cinq ans et d'une amende de cinq à cent millions de Francs congolais ou d'une de ces peines seulement.

Si les faits visés aux alinéas précédents ont été commis au préjudice d'une personne dont la situation de vulnérabilité en raison de l'âge, d'un état de grossesse, d'une maladie, d'une infirmité ou d'une déficience physique ou mentale était apparente ou connue de l'auteur des faits, les peines prévues aux alinéas précédents pourront être portées au double.

SECTION 5 : DE LA FRAUDE AUX CARTES BANCAIRES ET DES INFRACTIONS RELATIVES A LA PUBLICITE SUR INTERNET

Paragraphe 1 : De la fraude aux cartes bancaires

Article 372.

Est puni d'une peine de servitude pénale de deux à cinq ans et d'une amende de cinq à vingt et cent millions de Francs congolais ou l'une de ces peines seulement, le fait pour toute personne de :

1) 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) 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) 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 373.

Est puni d'une peine de servitude pénale de cinq à dix ans et de cinq à dix millions de Francs congolais d'amende ou de l'une de ces peines seulement, 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 précédent.

La confiscation, aux fins de destruction des cartes de paiement contrefaites ou falsifiées est obligatoire dans les cas prévus ci-dessus. Est également obligatoire la confiscation des matières, machines, outils, 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.

Dans tous les cas prévus aux alinéas ci-dessus, l'autorité judiciaire peut prononcer, en cas de récidive, l'interdiction des droits civils ainsi que l'interdiction, pour une durée de deux ans au plus, d'exercer une activité professionnelle ou sociale.

Paragraphe 2 : Des infractions relatives à la publicité sur Internet

Article 374.

Le fait de faire de la publicité au moyen d'un ou sur un réseau de communication électronique ou un système informatique en faveur de jeux d'argent et de hasard sur internet non autorisés est interdit.

Quiconque contrevient à l'interdiction définie à l'alinéa 1, est puni d'une amende de vingt à cinquante millions de Francs congolais.

La juridiction compétente peut porter le montant de l'amende au quadruple du montant des dépenses publicitaires consacrées à l'opération illégale.

SECTION 6 : DES CONTENUS ABUSIFS

Paragraphe 1 : De la diffusion de matériel tribaliste, raciste et xénophobe par le biais d'un système informatique

Article 375.

Quiconque aura, intentionnellement, crée, téléchargé, diffusé ou mis à la disposition sous quelque forme que ce soit, par le biais d'un système informatique du matériel raciste ou xénophobe, au sens du présent Code et conformément aux dispositions de l'ordonnance-loi n° 66-342 du 07 juin 1966 portant répression du racisme et du tribalisme, sera puni d'une servitude pénale d'un mois à deux ans et d'une amende d'un million à dix millions de francs Congolais ou de l'une de ces peines seulement.

Paragraphe 2 : Du harcèlement par le biais d'une communication électronique

Article 376.

Quiconque initie une communication électronique qui contraint, intimide, harcèle ou provoque une détresse émotionnelle chez une personne, en utilisant un système informatique dans le but d'encourager un comportement haineux, tribal et hostile aux bonnes mœurs et aux valeurs patriotiques est puni d'une servitude pénale d'un mois à deux ans et d'une amende de cinq cent mille à dix millions de Francs congolais.

Article 377.

Quiconque aura harcelé, par le biais d'une communication électronique, une personne alors qu'il savait ou aurait dû savoir qu'il affecterait gravement par ce comportement la tranquillité de la personne visée, sera puni d'une servitude pénale d'un mois à deux ans et d'une amende de cinq cent mille à dix millions de Francs congolais, ou de l'une de ces deux peines seulement.

Article 378.

Quiconque initie ou relaie une fausse information contre une personne par le biais des réseaux sociaux ou toute forme de support électronique est puni d'une servitude pénale d'un à six mois et d'une amende de cinq cent mille à un million de Francs congolais ou de l'une de ces peines seulement.

Paragraphe 3 : De la négation, minimisation grossière, approbation ou justification des crimes internationaux

Article 379.

Est puni d'une servitude pénale de dix à vingt ans et d'une amende d'un million à dix millions de Francs congolais, quiconque diffuse ou met à disposition par le biais d'un système informatique des données qui nient, minimisent, approuvent ou justifient des actes constitutifs de crime de génocide, crimes de guerre, crimes contre l'humanité et crime d'agression tels que définis les instruments internationaux et le Code pénal congolais et reconnus comme tels par une décision finale et définitive d'un tribunal national ou international.

Paragraphe 4 : De l'incitation ou provocation à la commission d'actes terroristes et apologie des actes terroristes

Article 380.

Quiconque aura, au moyen d'un ou sur un réseau de communication électronique ou un système informatique, incité ou provoqué directement des actes de terrorisme, sera puni conformément aux dispositions des articles 157 à 160 du Code pénal militaire congolais.

Paragraphe 5 : Du courrier indésirable ou pourriel

Article 381.

Sera puni d'une servitude pénale de deux à cinq ans et d'une amende de dix à cinquante millions Francs congolais ou d'une de ces peines seulement toute personne qui, intentionnellement et sans motif ou justification légitime, ou en se prévalant à tort d'un motif ou d'une justification légitime :

1) déclenche la transmission des messages de courrier électronique multiples à partir ou par l'intermédiaire d'un système informatique ;

2) utilise un système informatique protégé pour relayer ou retransmettre des messages de courrier électronique multiples dans le but de tromper ou d'induire en erreur les utilisateurs ou tout fournisseur de service de courrier électronique ou d'accès à l'internet quant à l'origine de ces messages ;

3) falsifie gravement les informations d'en-tête dans des messages de courriers électroniques multiples et déclenche intentionnellement la transmission de ces messages.

SECTION 7 : DES INFRACTIONS A CHARGE DU FOURNISSEUR D'ACCES A INTERNET

Article 382.

Tout fournisseur d'accès à internet qui n'informe pas ses abonnés de l'existence de moyens techniques permettant de restreindre l'accès à certains services est puni d'une amende de cinq cent mille à deux millions de Francs congolais.

En cas de récidive l'amende est fixée à cinq millions de Francs congolais.

Article 383.

Toute personne qui signale à un fournisseur de services en ligne 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 que cette information est inexacte, est punie de six à douze mois de servitude pénale et d'une amende de trois à cinq millions de Francs congolais ou de l'une de ces peines seulement.

Article 384.

Toute personne physique ou tout dirigeant d'une personne morale, de droit ou de fait, exerçant l'activité de fournisseur d'accès à internet ou de fournisseur de services en ligne, qui ne satisfait pas à l'une des obligations prévues au Titre 1 du présent Livre, est puni d'une servitude pénale de six à douze mois et d'une amende de dix à cinquante millions de Francs congolais ou l'une de ces peines seulement.

Est puni d'une servitude pénale de six à douze mois et d'une amende de dix à cinquante millions de Francs congolais ou de l'une de ces peines seulement, le fait, pour une personne physique ou un dirigeant d'une personne morale, de droit ou de fait, exerçant l'activité d'éditeur de services de communication en ligne, de ne pas avoir respecté l'obligation de vigilance prévue au Livre V du présent Code.

SECTION 8 : DES INFRACTIONS DE PRESSE EN LIGNE ET DE LA DIVULGATION DES DÉTAILS D'UNE ENQUÊTE

Paragraphe 1 : Des infractions de presse par le biais d'une communication électronique et droit de réponse

Article 385.

Quiconque aura commis des actes constitutifs d'une infraction de presse, par le biais d'un moyen de communication électronique public, sera puni des mêmes peines que celles prévues par la loi en vigueur, quel qu'en soit l'outil utilisé.

Article 386.

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 de demande de correction ou de suppression du message qu'elle peut adresser au service.

La demande de correction ou de suppression est présentée au plus tard dans un délai de trois mois à compter de la mise à disposition du public du message la justifiant.

Le Directeur de la publication est tenu d'insérer dans les trois jours de leur réception, les réponses de toute personne nommée ou désignée dans les services de communication en ligne.

A défaut de respecter le prescrit de l'alinéa précédent, le Directeur de la publication sera puni d'une amende de deux à cinq cent mille Francs congolais.

Paragraphe 2 : De la divulgation des détails d'une enquête

Article 387.

Est puni d'une servitude pénale d'un mois à deux ans, ou d'une amende deux à cinq millions de Francs congolais ou de l'une de ces peines seulement, un fournisseur de services qui, dans le cadre d'une enquête pénale, reçoit une injonction stipulant explicitement que la confidentialité doit être maintenue, ou lorsqu'une telle obligation est énoncée par la loi, et qui, sans motif ou justification légitime, ou en se prévalant à tort d'un motif ou d'une justification légitime, divulgue de manière intentionnelle :

1) le fait qu'une injonction ait été émise ;
2) toute action réalisée aux termes de l'injonction ;
3) toute donnée collectée ou enregistrée aux termes de l'injonction.

SECTION 9 : DE L'ESPIONNAGE ECONOMIQUE

Article 388.

Sera puni d'une servitude pénale de cinq à quinze ans et d'une amende de cinq à dix milliards de Francs congolais, ou de l'une de ces peines seulement, quiconque, ayant l'intention ou sachant que l'infraction profite à un gouvernement étranger, à un intermédiaire étranger, ou à un agent étranger qualifié d'espion :

1. vole, ou, sans autorisation, s'approprie, prend, emporte, ou cache, ou frauduleusement, ou de façon factice, ou par supercherie, obtient un secret commercial ;
2. sans autorisation, copie, duplique, illustre, dessine, photographie, télécharge, modifie, détruit, photocopie, reproduit, transmet, livre, envoie, adresse par courrier, communique ou cède un secret commercial ;
3. reçoit, achète, ou possède un secret commercial, sachant que ce dernier a été volé ou approprié, obtenu ou transformé sans autorisation ;
4. tente de commettre une infraction décrite à l'un des paragraphes 1 à 3 ;
5. conspire avec une ou plusieurs personnes en vue de commettre une infraction décrite à l'un des paragraphes 1 à 3 et qu'une ou plusieurs de ces personnes agissent de façon à obtenir l'objet de la conspiration.

Toute organisation qui commet une infraction décrite à l'alinéa précédent est punie d'une amende de quinze à vingt milliards de Francs congolais.

SECTION 10 : DE L'ENREGISTREMENT DES IMAGES RELATIVES A LA COMMISSION DES INFRACTIONS ET DE LA DIFFUSION DES ELEMENTS POUR FABRIQUER DES ENGINS DE DESTRUCTION

Paragraphe 1 : De l'enregistrement des images relatives à la commission des infractions

Article 389.

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.

Est puni d'une servitude pénale d'un à cinq ans et d'une amende de vingt à vingt-cinq millions de Francs congolais, toute personne qui diffuse sciemment de telles images.

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.

Paragraphe 2 : De la diffusion des éléments pour fabriquer des engins de destruction

Article 390.

Quiconque aura diffusé, au moyen d'un réseau de communication électronique ou d'un système informatique, sauf à des fins professionnelles, 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, sera puni de cinq à dix ans de servitude pénale et d'une amende de vingt-cinq millions de Francs congolais.

Lorsque ces procédés ont permis la commission de meurtre ou d'assassinat, la peine est de vingt ans de servitude pénale et d'une amende de cinquante à cent millions de Francs congolais.

Paragraphe 3 : De l'omission d'entretenir les dispositifs de protection

Article 391.

Est puni d'une amende de dix à cinquante millions de Francs congolais, le fait pour les mêmes personnes, d'omettre maintenir en bon état les dispositifs de protection.

SECTION 11 : DE L'ATTEINTE AUX DROITS D'AUTEUR ET A LA PROPRIETE INTELLECTUELLE ET INDUSTRIELLE

Article 392.

Sans préjudice de l'article 4 de l'ordonnance-loi 86-033 du 5 avril 1986 portant protection des droits d'auteurs et des droits voisins en République Démocratique du Congo, constituent également les œuvres de l'esprit protégées par la présente loi notamment : les logiciels, les applications, les plateformes numériques, y compris le matériel de conception préparatoire.

Paragraphe 1 : De la contrefaçon de marque, nom commercial, appellation d'origine, indication géographique, logiciel et matériel de conception préparatoire

Article 393.

La contrefaçon de marque, de nom commercial, d'appellation, de logiciel, des matériels de conception préparatoire et d'indication géographique est punie d'une peine de servitude pénale de cinq à dix ans et d'une amende de cinquante à cent millions de Francs congolais ou de l'une de ces peines seulement.

Constitue la contrefaçon, le fait sans autorisation de l'auteur ou de ses ayants droit, de reproduire, d'utiliser, de vendre, de dénigrer, de dénaturer une marque, un nom commercial,

une appellation d'origine ou une indication géographique appartenant à autrui au moyen d'un ou sur un réseau de communication électronique ou un système informatique.

Paragraphe 2 : De la contrefaçon de dessins et modèles

Article 394.

Est puni d'une servitude pénale de trois à cinq ans et d'une amende de cinquante à cent millions de Francs congolais ou d'une de ces peines seulement celui qui, sans autorisation de l'auteur ou de ses ayants droit, de reproduire, de 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 réseau de communication électronique ou un système informatique.

Paragraphe 3 : De l'atteinte aux droits de propriété des brevets

Article 395.

Constitue une atteinte à la propriété intellectuelle 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 réseau de communications électroniques.

Ceux qui, avec connaissance, vendent, exposent en vente, donnent en location, détiennent ou introduisent sur le territoire de la République Démocratique du Congo dans un but commercial, des objets ou des ouvrages ou des logiciels ou des matériels informatiques protégés par un brevet d'invention sont punis des mêmes peines prévues à l'article 14 du Code pénal.

Paragraphe 4 : De l'atteinte aux schémas de configuration d'un système numérique

Article 396.

Constitue une atteinte à la propriété intellectuelle, 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 d'un système numérique au moyen d'un réseau de communications électroniques.

Paragraphe 5 : De l'atteinte à une mesure technique efficace

Article 397.

Est puni d'une amende de deux cents à sept cent mille Francs congolais, le fait de porter atteinte sciemment, à des fins autres que la recherche, à une mesure technique efficace afin d'altérer la protection d'un matériel par un décodage, un décryptage ou toute autre intervention personnelle destinée à contourner, neutraliser ou supprimer un mécanisme de protection ou de contrôle,

lorsque cette atteinte est réalisée par d'autres moyens que l'utilisation d'une application technologique ou d'un dispositif.

Est puni de six mois à un an de servitude pénale et d'une amende de deux à cinq cent mille Francs congolais ou de l'une de ces peines seulement, le fait de procurer ou proposer sciemment à autrui, directement ou indirectement, des moyens conçus ou spécialement adaptés pour porter atteinte à une mesure technique efficace, par l'un des procédés suivants :

1. en fabriquant ou en important une application technologique ou un dispositif à des fins autres que la recherche ;
2. en détenant en vue de la vente, du prêt ou de la location, en offrant à ces mêmes fins ou en mettant à disposition du public sous quelque forme que ce soit, une application technologique, un dispositif ou un composant ;
3. en fournissant un service à cette fin ;
4. en incitant à l'usage ou en commandant, concevant, organisant, reproduisant, distribuant ou diffusant une publicité en faveur de l'un des procédés visés aux points 1 à 3 au moyen d'un réseau de communications électroniques.

Ces dispositions ne sont pas applicables aux actes réalisés à des fins de sécurité informatique.

Paragraphe 6 : De la suppression d'un élément d'information sur le régime des droits pour porter atteinte au droit d'auteur

Article 398.

Est puni d'une amende de deux à cinq millions de Francs congolais au maximum, le fait de supprimer ou de modifier, sciemment et à des fins autres que la recherche, tout élément d'information sur le régime des droits, par une intervention personnelle, dans le but de porter atteinte à un droit d'auteur, de dissimuler ou de faciliter une telle atteinte.

Est puni d'une servitude pénale de deux à six mois et d'une amende de deux à cinq millions de Francs congolais, ou de l'une de ces peines seulement, le fait de procurer ou de proposer sciemment à autrui, directement ou indirectement, des moyens conçus ou spécialement adaptés pour supprimer ou modifier, même partiellement, un élément d'information sur le régime des droits, dans le but de porter atteinte à un droit d'auteur, de dissimuler ou de faciliter une telle atteinte, par l'un des procédés suivants :

1. en fabriquant ou en important une application technologique, un dispositif ou un composant, à des fins autres que la recherche ;
2. en détenant en vue de la vente, du prêt ou de la location, en offrant à ces mêmes fins ou en mettant à disposition du public sous quelque forme que ce soit une application technologique, un dispositif ou un composant ;
3. en fournissant un service à cette fin ;

4. en incitant à l'usage ou en commandant, concevant, organisant, reproduisant, distribuant ou diffusant une publicité en faveur de l'un des procédés visés aux points 1 à 3 au moyen d'un système d'information.

Est puni d'une servitude pénale de deux à six mois et d'une amende de deux cents à cinq cent mille Francs congolais, ou de l'une de ces peines seulement, le fait d'importer, de distribuer, de mettre à disposition du public sous quelque forme que ce soit ou de communiquer au public, directement ou indirectement, une œuvre dont un élément d'information sur le régime des droits a été supprimé ou modifié dans le but de porter atteinte à un droit d'auteur, de dissimuler ou de faciliter une telle atteinte.

Ces dispositions ne sont pas applicables aux actes réalisés à des fins de recherche ou de sécurité informatique.

Paragraphe 7 : De l'altération

Article 399.

Est puni d'une amende de deux cents à sept cent mille Francs congolais, le fait de porter atteinte sciemment, à des fins autres que la recherche, à une mesure technique efficace afin d'altérer la protection d'une interprétation, d'un phonogramme, d'un vidéogramme ou d'un programme par un décodage, un décryptage ou toute autre intervention personnelle destinée à contourner, neutraliser ou supprimer un mécanisme de protection ou de contrôle, lorsque cette atteinte est réalisée par d'autres moyens que l'utilisation d'une application technologique, d'un dispositif ou d'un composant existant prévu au chapitre II du présent Livre.

Est puni d'une servitude pénale de deux à six mois et d'une amende de deux cent mille à cinq cent mille Francs congolais, ou de l'une de ces peines seulement, le fait de procurer ou de proposer sciemment à autrui, directement ou indirectement, des moyens conçus ou spécialement adaptés pour porter atteinte à une mesure technique efficace, par l'un des procédés suivants :

1. en fabriquant ou en important une application technologique, un dispositif ou un composant, à des fins autres que la recherche ;
2. en détenant en vue de la vente, du prêt ou de la location, en offrant à ces mêmes fins ou en mettant à disposition du public sous quelque forme que ce soit une application technologique, un dispositif ou un composant ;
3. en fournissant un service à cette fin ;
4. en incitant à l'usage ou en commandant, concevant, organisant, reproduisant, distribuant ou diffusant une publicité en faveur de l'un des procédés visés aux points 1 à 3.

Ces dispositions ne sont pas applicables aux actes réalisés à des fins de sécurité informatique.

Est puni d'une amende de dix millions de francs congolais au maximum, le fait pour les mêmes personnes, d'omettre d'entretenir en bon état, les dispositifs de protection antérieurement établis.

LIVRE VII : DES DISPOSITIONS DIVERSES, TRANSITOIRES ET FINALES

CHAPITRE I : DU REGIME FISCAL, PARAFISCAL, DOUANIER ET DE CHANGE

Article 400.

Les personnes morales et physiques évoluant dans le secteur du numérique sont soumises au régime du droit commun en matière fiscale, parafiscale, douanière et de change en vigueur.

Article 401.

Les startups du numérique, ayant le statut d'entreprenant, sont éligibles aux avantages fiscaux, parafiscaux, douanier et de change prévus par la législation relative à l' entrepreneuriat et aux startups.

En outre et sans préjudice des dispositions de l'Ordonnance-loi nº 69-006 du 10 février 1969 portant sur l'impôt réel telle que modifiée à ce jour et d'autres textes applicables en matière fiscale :

1) il est accordé aux startups, aux personnes physiques ayant le statut d'entreprenant ainsi qu'aux petites et moyennes entreprises évoluant dans le secteur du numérique, une exonération totale des impôts, droits, taxes et redevances pour une période de douze mois, deux fois renouvelable, à l'exception des impôts, droits, taxes et redevances dont elles sont redevables légales ou ceux perçus en contrepartie des services rendus ;

2) Il est accordé aux fournisseurs de services numériques que ceux repris au point ci-dessus, un allègement de 50 % de l'impôt sur les bénéfices et profits, des droits de douane à l'importation des équipements destinés à l'exploitation des services numériques, des droits d'accises sur les services numériques, des impôts, droits, taxes et redevances ainsi qu'autres impôts, droits, taxes et redevances indirects pour une période de cinq ans. Exception faite des impôts professionnels sur les rémunérations et mobiliers.

Article 402.

Un arrêté des Ministres ayant les finances, les petites et moyennes entreprises et le numérique dans leurs attributions définit les critères d'éligibilité au régime dérogatoire prévu à l'article 410 du présent Code.

Article 403.

L'admission à un des régimes juridiques prévus dans le présent Code n'est effective qu'après paiement par le fournisseur ou le prestataire des services numériques, selon le cas, des droits, taxes et redevances dus à l'Etat.

Il est ajouté une annexe relative aux droits, taxes et redevances dus au secteur du numérique en complément à l'Ordonnance-loi nº 18/003 du 13 mars 2018 fixant la nomenclature des droits, taxes et redevances du pouvoir central, ainsi libellée :

XXXII. NUMERIQUE

Nº	LIBELLE DES DROITS, TAXES ET REDEVANCES	FAIT GENERATEUR
01	Taxe sur l'autorisation en vue de la fourniture des services numériques 1. fourniture de services numériques de confiance qualifiée ; 2. fourniture de services d'hébergement des applications financières ; 3. fourniture de services numériques par des opérateurs de télécommunications.	Demande d'autorisation
02	Taxe sur la déclaration en vue d'un certificat d'agrément en fourniture des services numériques	Demande d'un certificat d'agrément
03		
04		
05		
06		
07		

Un arrêté interministériel des Ministres ayant le numérique et les finances dans leurs attributions fixe les taux des droits, taxes et redevances à percevoir à l'initiative du ministère du numérique.

CHAPITRE II : DE COMMANDE PUBLIQUE

Article 404.

La passation d'un marché public est régie conformément à la section 5 de la loi nº 10/010 du 27 avril 2010 relative aux marchés publics.
L'établissement d'un partenariat public-privé est régi conformément Loi n°18/016 du 09 juillet 2018 relative au partenariat public-privé.

Article 405.

Les fournisseurs des services numériques opérant sur base des titres obtenus antérieurement au présent Code sont tenus de se conformer aux nouvelles dispositions du présent Code dans un délai de six mois à dater de son entrée en vigueur.

Article 406.

Un décret du Premier Ministre, délibéré en Conseil des Ministres, fixe les mesures d'application du présent Code.

CHAPITRE III : DES DISPOSITIONS FINALES

Article 407.

Sont abrogées :

1. les titres III et IV de la loi n° 20/017 du 25 novembre 2020 relative aux télécommunications et aux technologies de l'information et de la communication ainsi que toute autre disposition de la même loi se rapportant aux activités et services numériques ;
2. toute disposition contraire au présent Code.

Article 408.

Le présent Code entre en vigueur à la date de sa promulgation.

Fait à Kinshasa, le

Félix Antoine TSHISEKEDI TSHILOMBO

TABLE DE MATIÈRES