RÉPUBLIQUE DÉMOCRATIQUE DU CONGO

Justice – Paix – Travail

MINISTÈRE DE L'ÉCONOMIE NUMÉRIQUE

Cabinet du Ministre

ORDONNANCE-LOI N° 23/010 DU 13 MARS 2023

PORTANT

CODE DU NUMÉRIQUE

Édition de diffusion du Ministère de l'Économie Numérique

Kinshasa, octobre 2026

PLAN SOMMAIRE DU CODE

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

LIVRE PREMIER — DES ACTIVITÉS ET DES SERVICES NUMÉRIQUES

LIVRE II — DES ÉCRITS, DES OUTILS ÉLECTRONIQUES ET DES PRESTATAIRES DE SERVICES DE CONFIANCE

LIVRE III — DES CONTENUS NUMERIQUES

LIVRE IV — DE LA SÉCURITÉ ET DE LA PROTECTION PÉNALE DES SYSTÈMES INFORMATIQUES

LIVRE V — DES DISPOSITIONS DIVERSES, TRANSITOIRES, ABROGATOIRES ET FINALES

Le Président de la République,

Vu la Constitution, telle que modifiée par la Loi n° 11/002 du 20 janvier 2011 portant révision de certains articles de la Constitution de la République Démocratique du Congo du 18 février 2006, spécialement en ses articles 31 et 129 ;

Vu la Loi n° 22/060 du 27 décembre 2022 portant habilitation du Gouvernement, spécialement en ses articles 1er, 2 et 3 ;

Vu l'Ordonnance n° 22/002 du 07 janvier 2022 portant organisation et fonctionnement du Gouvernement, modalités de collaboration entre le Président de la République et le Gouvernement ainsi qu'entre les Membres du Gouvernement, spécialement en ses articles 45 et 46 ;

Vu l'Ordonnance n° 21/006 du 14 février 2021 portant nomination d'un Premier Ministre ;

Vu l'Ordonnance n° 21/012 du 12 avril 2021 portant nomination des Vice-Premiers Ministres, des Ministres d'État, des Ministres, des Ministres Délégués et des Vice-Ministres ;

Vu la nécessité et l'urgence

Sur proposition du Gouvernement, délibérée en Conseil des Ministres ;

ORDONNE :

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

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

Article 1.

La législation du numérique est constituée par la présente ordonnance-loi et les dispositions légales et réglementaires édictées pour son application.

La présente ordonnance-loi s'applique :

1. aux activités et services numériques ;
2. aux écrits, outils électroniques et prestataires de services de confiance ;
3. aux contenus numériques ;
4. à la sécurité et à la protection pénale des systèmes informatiques.

En outre, elle fixe le régime fiscal, parafiscal, douanier et de change applicable aux activités et services numériques en République Démocratique du Congo.

CHAPITRE II : DES DEFINITIONS

Article 2.

Au sens de la présente ordonnance-loi, on entend par :

1. **Accès** : connexion directe ou indirecte dans l'intégralité ou dans une partie quelconque d'un système informatique via un réseau de communication électronique ;

2. **Adresse** : élément de localisation physique et/ou électronique ;

3. **Archivage** : opération consistant à organiser et à conserver des archives aux fins d'une utilisation ultérieure, que cette conservation soit administrative ou historique ;

4. **Archivage électronique** : archivage qui consiste à mettre en place des actions, outils et méthodes afin de conserver des données, des documents et des informations à long terme et au format dématérialisé et de manière sécurisée en vue d'une éventuelle utilisation ultérieure ;

5. **Archives** : documents, quels que soient leurs dates, leurs formats et leurs supports, produits ou reçus et délibérément conservés par toute personne, physique ou morale, publique ou privée ;

6. **Autorisation** : acte administratif d'une Autorité Compétente qui confère à son bénéficiaire un ensemble de droits et d'obligations spécifiques concernant l'exercice d'une activité déterminée conformément à la présente ordonnance-loi ;

7. **Autorité compétente** : autorité désignée par voie légale ou réglementaire exerçant une mission de valeur dans ses compétences en vertu de la présente ordonnance-loi ou de toute autre loi ;

8. **Cachet électronique** : donnée électronique, jointe ou associée logiquement à d'autres données électroniques afin de garantir l'originalité et l'intégrité de ces dernières ;

9. **Cahier des charges** : document intégrant les conditions organisationnelles, techniques, opérationnelles et les modalités d'exploitation imposées à tout opérateur et/ou fournisseur de services numériques ;

10. **Catégories particulières de données** : données qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que les données génétiques, les données biométriques aux fins d'identifier une personne physique de manière unique, y compris les données concernant la santé et les données concernant la vie sexuelle, les mineurs et les condamnations judiciaires ;

11. **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 ;

12. **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 ;

13. **Certificat qualifié de cachet électronique** : acte délivré par un prestataire de services de confiance qualifié et qui satisfait aux exigences légales ;

14. **Certificat qualifié de signature électronique** : acte délivré par un prestataire de services de confiance qualifié et qui satisfait aux exigences légales ;

15. **Commerce électronique** : activité commerciale par laquelle une personne propose ou assure par voie électronique ou via un système informatique, moyennant paiement d'un prix, la fourniture de biens ou de services ;

16. **Communication électronique** : émission, transmission et 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 ;

17. **Confidentialité** : état de sécurité permettant de garantir le secret des informations, des données et des ressources stockées vis-à-vis des tiers non autorisés ;

18. **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 ;

19. **Conservation des données** : sauvegarde des données dans l'état dans lequel elles se trouvent ;

20. **Consommateur ou usager** : utilisateur des activités et/ou services numériques ;

21. **Contenu numérique** : ensemble de données, de programmes informatiques, des applications mobiles ou web ainsi que des fichiers audio, vidéo, texte, sous forme numérique ;

22. **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 ;

23. **Cryptographie** : ensemble des principes, moyens et méthodes de transformation des données, dans le but de cacher leur contenu, d'empêcher que leur modification ne passe inaperçue et/ou d'empêcher leur utilisation non autorisée ;

24. **Cybercriminalité** : ensemble des infractions pénales spécifiques liées aux technologies de l'information et de la communication telles que définies par la présente ordonnance-loi, ainsi que celles prévues dans d'autres lois particulières, dont la commission est facilitée ou liée à l'utilisation des technologies ;

25. **Cybersécurité** : ensemble des mesures de prévention, de protection et de dissuasion d'ordre technique, organisationnel, juridique, financier, humain et procédural ou autre permettant d'atteindre les objectifs de sécurité des systèmes informatiques et des réseaux de communication électronique et de garantir la disponibilité, l'intégrité, la confidentialité, l'authenticité ou la traçabilité des données stockées, traitées ou transmises et des services connexes ;

26. **Déclaration** : acte préalable à toute activité émanant d'un opérateur ou d'un fournisseur de services numériques conformément aux dispositions de la présente ordonnance-loi ;

27. **Destinataire** : personne habilitée à recevoir la communication des données autre que la personne concernée, le responsable du traitement du le sous-traitant et les personnes qui, en raison de leurs fonctions, sont chargées de traiter les données ;

28. **Donnée** : information ou ensemble d'informations susceptible d'être stockée, traitée ou analysée au sein d'un système informatique ou d'un réseau de communication électronique ;

29. **Donnée biométrique** : donnée qui se rapporte aux caractéristiques physiques, biologiques ou comportementales permettant d'identifier une personne physique telles que les empreintes digitales, les images faciales, la voix, l'iris ou la démarche ;

30. **Donnée personnelle ou donnée à caractère personnel** : toute information se rapportant à une personne physique identifiée ou identifiable directement ou indirectement ;

31. **Donnée publique** : donnée produite, gérée et stockée dans les registres publics de données sur le territoire de la République démocratique du Congo dans le cadre d'une mission de service public par l'État, les provinces, les entités territoriales, les services, établissements et organismes publics ainsi que les personnes morales de droit privé chargées d'une mission de service public ;

32. **Donnée sensible** : donnée biométrique, donnée à caractère personnel relative notamment aux origines raciales ou ethniques, aux opinions ou activités politiques, aux convictions religieuses ou philosophiques, aux appartenances syndicales, à la vie sexuelle, à la santé, à la génétique ;

33. **Donnée stratégique** : donnée des personnes morales publiques ou privées, institutionnelle ou professionnelle, relative à la sûreté de l'État, à valeur économique ou sécuritaire dont la fuite, l'altération, la suppression et/ou l'utilisation frauduleuse serait préjudiciable aux institutions, organisations ou professions concernées ;

34. **Fichier** : répertoire structuré des données numériques, centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique ;

35. **Fournisseur de services en ligne** : personne physique ou morale offrant des services via Internet conformément à la présente ordonnance-loi ;

36. **Fournisseur de services numériques** : personne physique ou morale opérant dans le secteur des activités et services numériques conformément à la présente ordonnance-loi ;

37. **Hameçonnage ou phishing** : technique de manipulation par tromperie utilisée par les pirates informatiques visant à récupérer auprès d'un utilisateur ou d'un système informatique ou d'un réseau de communication électronique, des informations ou des données à caractère personnel ;

38. **Hébergeur** : personne physique ou morale qui fournit un service de transmission électronique d'informations en stockant les données fournies par l'utilisateur du service ;

39. **Horodatage électronique** : opération visant à associer à un fichier sa date et son heure de création ou de réception conformément aux dispositions de la présente ordonnance-loi ;

40. **Horodatage électronique certifié** : horodatage électronique qui satisfait aux exigences fixées par la présente ordonnance-loi et généré par un prestataire de services de confiance qualité ;

41. **INACO** : Institut National des Archives du Congo ;

42. **Identification électronique** : processus qui consiste à l'utilisation des données et éléments constitutifs de l'identité d'une personne physique ou morale par des procédés électroniques qui représentent de manière univoque la personne physique ou morale concernée ;

43. **Infrastructure critique ou essentielle** : ensemble d'installations, de ressources, d'équipements et/ou de services, non-interchangeables aux caractéristiques particulières qui, en raison du coût prohibitif de leur reproduction, il serait impossible, pour les concurrents potentiels, de les reproduire par des moyens raisonnables ;

44. **Intégrité** : état de sécurité assurant qu'un réseau de communications électroniques, système informatique 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 ;

45. **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 informatiques 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 ;

46. **Interopérabilité** : capacité de collaboration et de communication entre deux ou plusieurs systèmes informatiques, services ou contenus numériques ;

47. **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 contenu ou toute autre information lorsqu'elle est exécutée ;

48. **Limitation du traitement** : mécanisme consistant à ne traiter que des données qui sont utiles à une finalité déterminée ;

49. **Logiciel** : ensemble de programmes ou procédures nécessaires au fonctionnement d'un système informatique ou d'un réseau de communication électronique ;

50. **Market place** : plateforme qui met en relation des acheteurs et des vendeurs dans un système informatique ou un réseau de communication électronique ;

51. **Message électronique** : information envoyée ou transmise à travers un système informatique ou un réseau de communication électronique ;

52. **Moyen d'identification électronique** : élément matériel et/ou immatériel contenant des données d'identification des personnes physiques ou morales ;

53. **Neutralité technologique** : obligation pour la législation du numérique d'être non-discriminatoire entre les opérateurs du secteur ;

54. **Normes et Standards du Numérique applicables au secteur public** : ensemble de bonnes pratiques gouvernementales, de référentiels et directives techniques, spécifiant notamment l'architecture des systèmes de gestion de données de l'État, des entités territoriales et autres personnes publiques, le niveau de sécurité et les normes d'interopérabilité des systèmes informatiques du secteur public de la République Démocratique du Congo ;

55. **Numérique** : ensemble des procédés et moyens utilisant des outils et services qui permettent de créer, de traiter, de stocker et de diffuser la donnée ;

56. **Opérateurs d'importance vitale (OIV)** : opérateurs publics ou privés exploitant des établissements ou utilisant des installations et ouvrages, dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation ;

57. **Personne concernée** : personne physique qui fait l'objet d'un traitement des données et qui est identifiée ou identifiable ;

58. **Plainte** : 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 ;

59. **Pourriel ou spam** : courrier électronique indésirable, non sollicité par le destinataire ;

60. **Prestataire de service de confiance** : personne physique ou morale qui fournit un ou plusieurs services de confiance conformément à la présente ordonnance-loi ;

61. **Prestataire de services de confiance qualifiée** : prestataire chargé de vérifier l'identité d'une personne physique ou morale pour pouvoir émettre un certificat électronique en sa faveur conformément à la présente ordonnance-loi ;

62. **Profilage** : technique d'analyse de données personnelles qui permet de créer des profils et/ou des modèles pour identifier les caractéristiques ou les comportements d'un groupe ou d'un individu ;

63. **Prospection directe** : 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 ;

64. **Registre National de la Population** : fichier général de la population ;

65. **Registre public des données** : base de données contenant diverses informations récoltées par des systèmes sectoriels qui participent à la gouvernance numérique ;

66. **Représentant du responsable de traitement** : personne physique ou morale établie de manière stable sur le territoire du pays, qui se substitue au responsable de traitement dans l'accomplissement des obligations prévues par la présente ordonnance-loi ;

67. **Réseau de communication électronique** : installation ou ensemble d'installations de transport ou de diffusion ainsi que, le cas échéant, les autres moyens assurant l'acheminement de communications électroniques et les réseaux assurant la diffusion ou utilisés pour la distribution de services de communication ;

68. **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 ;

69. **Schéma d'identification électronique** : système ou processus pour l'identification électronique 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 ;

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

71. **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 ;

72. **Service ou activité numérique** : prestation proposée et/ou fournie au moyen d'un système informatique ou d'un réseau de communication électronique en vue notamment de créer, de traiter, de stocker ou de diffuser les données ;

73. **Services de communications électroniques** : 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 ;

74. **Signature électronique** : mécanisme permettant de garantir l'intégrité et la non-répudiation d'un document, et d'en authentifier de manière certaine l'auteur et d'apporter la preuve de son consentement, conformément aux dispositions de la présente ordonnance-loi ;

75. **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 ;

76. **Sous-traitance** : activité ou opération effectuée par une entreprise dite sous-traitante, 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 ;

77. **Souveraineté numérique** : droit d'autodétermination dont un pays dispose à décider de sa propre politique en matière du numérique notamment sur ses infrastructures, sur ses données et leurs traitements ;

78. **Système informatique** : dispositif composé de procédures, de matériels et de logiciels permettant l'échange, le stockage ou le traitement automatisé de données ;

79. **Table de correspondance** : liste d'association de valeurs informatiques ou électroniques ;

80. **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 ;

81. **Traitement** : 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 ;

82. **Transactions électroniques** : échanges sécurisés effectués lors d'un achat ou d'un paiement en ligne ;

83. **Utilisateur ou usager** : consommateur des services numériques ;

LIVRE PREMIER : DES ACTIVITÉS ET DES SERVICES NUMÉRIQUES

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

Article 3.

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 4.

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 réglementation et la régulation du secteur de l'audiovisuel.

TITRE II : DU CADRE INSTITUTIONNEL

Article 5.

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 du Numérique ;
3. l'Autorité Nationale de Certification Électronique ;
4. l'Agence Nationale de Cybersécurité ;
5. le Conseil National du Numérique.

L'organisation, le fonctionnement et les compétences de l'Agence Nationale de Cybersécurité sont mentionnés dans les dispositions du Livre IV de la présente ordonnance-loi.

CHAPITRE I : DU MINISTERE

Article 6.

Sans préjudice des missions prévues dans 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.

CHAPITRE II : DE L'AUTORITE DE REGULATION DU NUMERIQUE

Article 7.

L'Autorité de Régulation du Numérique est un établissement public créé par décret du Premier Ministre, délibéré en Conseil des Ministres et placée sous la tutelle du Ministre ayant le numérique dans ses attributions.

Les missions de régulation des activités et services du numérique sont assurées par l'Autorité de Régulation du Numérique, désignée par le sigle ARN.

L'Autorité de Régulation du Numérique 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, l'équité et la transparence en assurant l'équilibre du marché du secteur du numérique et de prendre toutes les mesures nécessaires aux fins de rétablir la concurrence au profit des usagers, et trancher les litiges ;
5. assurer la police des activités et des services du secteur du numérique ;
6. promouvoir et développer les activités dans le secteur du numérique ;
7. veiller au respect des obligations spécifiques qui s'imposent aux plateformes et fournisseurs en position dominante ;
8. assurer la participation aux activités de recherche, de formation et d'étude relatives aux échanges et au commerce électroniques ;
9. contribuer à la recherche, à la mobilisation et à la canalisation des financements nécessaires à la réalisation de l'éclosion du secteur et à la réduction de la fracture numérique ;
10. assurer la mission de prévention et de répression à l'encontre des plateformes et fournisseurs en position dominante après analyse de l'état et de l'évolution prévisible des aspects de la concurrence du marché.

Article 8.

Une quotité du fonds de service universel prévu par la loi n° 20/017 du 25 novembre 2020 relative aux télécommunications et aux technologies de l'information et de la communication sera affectée notamment à la promotion et au développement des activités et services numériques.

CHAPITRE III : DE L'AUTORITE NATIONALE DE CERTIFICATION ÉLECTRONIQUE

Article 9.

Il est créé, par décret du Premier Ministre délibéré en Conseil des Ministres, une Autorité de Certification Électronique dénommée Autorité Nationale de Certification Électronique, « ANCE » en sigle.

L'Autorité Nationale de Certification Électronique est un établissement public à caractère technique, placé sous la tutelle du Ministre ayant le numérique dans ses attributions.

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

Article 10.

L'Autorité Nationale de Certification Électronique a pour mission d'assurer le rôle de l'Autorité de Certification Électronique des activités et services numériques.

Sans préjudice des compétences spécifiques dévolues à certains services publics particuliers, l'Autorité Nationale de Certification Électronique est chargée de :

1. donner des avis aux requêtes d'exercice des activités des fournisseurs de services de confiance sur toute l'étendue du territoire national ;
2. assurer le contrôle du respect par les fournisseurs de services de certification électronique des dispositions de la présente ordonnance-loi et de ses mesures d'applications ;
3. fixer les caractéristiques du dispositif de création et de vérification de la signature électronique, du cachet électronique, de l'archivage électronique, de l'horodatage électronique et de l'authentification des sites Internet ;
4. gérer l'infrastructure à clés publiques nationales ;
5. émettre, délivrer et conserver des certificats électroniques des agents publics habilités à effectuer des échanges électroniques.

CHAPITRE IV : DU CONSEIL NATIONAL DU NUMERIQUE

Article 11.

Il est créé un organisme consultatif appelé Conseil National du Numérique (CNN) en sigle dont l'organisation et au fonctionnement sont fixés par Ordonnance du Président de la République.

Le CNN est placé sous l'autorité du Président de la République.

Il comprend une représentation de l'ensemble des acteurs du secteur du numérique, à savoir la Présidence de la République, le Gouvernement et ses services, le secteur privé, le Parlement, le monde scientifique, les Cours, tribunaux et parquets, la société civile ainsi que les autres parties prenantes.

Article 12.

Sans préjudice des attributions dévolues à d'autres organes, le Conseil National du Numérique a notamment pour mission de :

1. servir de cadre de concertation et d'évaluation des projets du Gouvernement dans le secteur du numérique ;
2. donner des avis au Gouvernement et mener des études sur les questions en relation avec le numérique ;
3. évaluer les politiques sectorielles et les initiatives des investissements numériques ;
4. veiller à l'éthique du numérique et principalement du numérique avancé, de l'Intelligence Artificielle, du Big Data, de la Robotique collaborative et du Blockchain ;
5. proposer et présenter au Gouvernement des initiatives sectorielles ainsi que les entraves à l'exécution des projets à caractère numérique.

TITRE III : DU RÉGIME JURIDIQUE APPLICABLE AUX ACTIVITÉS ET SERVICES NUMÉRIQUES

CHAPITRE I : DES DISPOSITIONS GENERALES

Article 13.

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

Sans préjudice des dispositions applicables aux sociétés commerciales, nul ne peut exercer une activité dans le secteur du numérique en République Démocratique du Congo, sans se soumettre à l'un des régimes juridiques prévus par la présente ordonnance-loi.

Article 14.

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

L'instruction des demandes d'autorisation ou de déclaration ainsi que l'élaboration du cahier des charges pour les prestataires de services de confiance relève de l'Autorité Nationale de Certification Électronique. L'instruction des demandes d'homologation de sécurité relève de l'Agence Nationale de Cybersécurité telle que prévue à l'article 278 livre IV de la présente ordonnance-loi.

CHAPITRE II : DE L'AUTORISATION

Article 15.

Sont soumis au régime d'autorisation :

1. les opérateurs et/ou fournisseurs de services numériques construisant des centres de données ;
2. les fournisseurs des services numériques de confiance qualifiée ;
3. les fournisseurs des services numériques essentiels ;
4. les fournisseurs des services d'hébergement d'applications, y compris celles financières ;
5. les plateformes numériques et les fournisseurs en position dominante œuvrant en République Démocratique du Congo.

Un Décret du Premier Ministre délibéré en Conseil des Ministres complète, sur proposition du Ministre ayant le numérique dans ses attributions, la liste des activités et services numériques soumis au régime d'autorisation, l'Autorité de Régulation du Numérique et l'Autorité Nationale de Certification Électronique entendues par avis écrit.

Article 16.

L'autorisation est délivrée par le Ministre ayant le numérique dans ses attributions après avis écrit de l'Autorité de Régulation du Numérique, de l'Autorité Nationale de Certification Électronique ou de l'Agence Nationale de Cybersécurité, selon les cas

CHAPITRE III : DE LA DECLARATION

Article 17.

Sont soumis au régime de déclaration :

1. les fournisseurs de services numériques de copies tampon ou serveurs cache des contenus des données ou médias d'autres fournisseurs ;

2. les opérateurs de points d'échange Internet ;

3. les développeurs des applications issues des startups congolaises.

Un arrêté du Ministre ayant le numérique dans ses attributions complète la liste des activités et services numériques soumis au présent régime de déclaration, l'Autorité de Régulation du Numérique entendue par avis écrit.

Article 18.

La déclaration est faite auprès de l'Autorité de Régulation du Numérique qui tient un registre public.

L'Autorité de Régulation du Numérique 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 IV : DE L'HOMOLOGATION

Article 19.

Le régime d'homologation atteste que les infrastructures et services numériques fournis à l'État sont conformes aux Normes et Standards du Numérique applicables au secteur public en République Démocratique du Congo ainsi qu'aux bonnes pratiques en la matière.

Sont soumis à l'homologation :

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.

Un Décret du Premier Ministre délibéré en Conseil des Ministres complète, sur proposition du Ministre ayant le numérique dans ses attributions, la liste des activités et services numériques soumis au régime d'homologation, l'Agence Nationale de Cybersécurité entendue par avis écrit.

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

Article 20.

Le certificat d'homologation est délivré par le Ministre ayant le numérique dans ses attributions après avis de l'Agence Nationale de Cybersécurité.

TITRE IV : DES DROITS, PRINCIPES GÉNÉRAUX ET OBLIGATIONS APPLICABLES AUX FOURNISSEURS DES ACTIVITÉS ET SERVICES NUMÉRIQUES

CHAPITRE I : DES DROITS ET PRINCIPES GÉNÉRAUX APPLICABLES AUX FOURNISSEURS DES ACTIVITÉS ET SERVICES NUMÉRIQUES

Article 21.

Sans préjudice des dispositions particulières, les activités et services numériques s'exercent librement, dans le respect des dispositions légales et réglementaires applicables en République Démocratique du Congo. Ils sont soumis aux principes ci-après :

1. Égalité de traitement ;
2. Transparence ;
3. Non-discrimination ;

4. Libre concurrence ;

5. Neutralité technologique.

Article 22.

Les fournisseurs de services numériques jouissent des mêmes droits et sont soumis aux mêmes obligations conformément aux dispositions de la présente ordonnance-loi.

À l'exception de la libre concurrence et de la neutralité technologique, les principes visés à l'article 21 ci-dessus s'appliquent également à toute autorité administrative, notamment à l'Autorité de Régulation du Numérique, à l'Autorité de Certification Électronique et à l'Agence Nationale de Cyber sécurité.

Article 23.

Les fournisseurs de services numériques intervenant sous un même régime juridique jouissent, dans les mêmes conditions, des 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 du Numérique.

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

Article 24.

L'Autorité de Régulation du Numérique et l'Autorité Nationale de Certification Électronique, selon les cas, veillent à l'application du principe de neutralité technologique.

Article 25.

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

Sous réserve 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 en droit international sont soumis aux dispositions de la présente ordonnance-loi.

Article 26.

En vue de la réalisation des travaux nécessaires à l'exploitation et à l'extension de leurs activités, les fournisseurs de 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 27.

Les accords entre fournisseurs de 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 de services numériques, ne peuvent limiter les droits acquis des utilisateurs en matière de fourniture des services.

Article 28.

L'Autorité de Régulation du Numérique et l'Autorité Nationale de Certification Électronique, selon les cas, veillent à la qualité et à la disponibilité permanente des services numériques fournis.

Elles imposent 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 de services numériques.

À la demande de l'Autorité de Régulation du Numérique ou de l'Autorité Nationale de Certification Électronique, les fournisseurs de services numériques mettent à leur disposition toute information relative à leurs obligations et communiquent ces informations dans les délais et selon le degré de précision exigés par elles.

CHAPITRE II : DES OBLIGATIONS DES FOURNISSEURS DES ACTIVITÉS ET SERVICES NUMÉRIQUES

Article 29.

Le fournisseur de 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 manière transparente ;
3. Fournir des services efficaces, fiables et conformes aux normes reconnues au niveau national, international fixées par l'Autorité de Régulation du Numérique ;
4. Publier par tout moyen d'information de masse et sans délai, 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 30.

Sous réserve des dispositions en la matière, toute personne physique ou morale qui remplit les conditions contractuelles et financières proposées par un fournisseur de services numériques ne peut se voir refuser la fourniture de ces services, s'il en a formulé la demande.

Le fournisseur de services numériques exige 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 subit pas d'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 31.

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 de services numériques dans leurs points de vente et par tout autre moyen de publicité.

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

Article 32.

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

L'Autorité de Régulation du Numérique précise les dispositions que doivent contenir les contrats à conclure avec les utilisateurs.

Article 33.

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

Article 34.

Le fournisseur de services numériques ne peut 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 la base d'un changement de la législation ou d'une décision de l'Autorité de Régulation du Numérique en application d'une disposition légale ou réglementaire.

Le 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 trente (30) jours ouvrables avant son entrée en vigueur, assorti de l'information selon laquelle les utilisateurs peuvent, tant qu'ils n'ont pas expressément accepté les nouvelles conditions, résilier le contrat sans pénalité de résiliation et sans droit au dédommagement, jusqu'à un délai de soixante (60) jours ouvrables après l'entrée en vigueur de la modification.

La modification ne prend effet qu'à l'issue de ce délai de soixante (60) jours ouvrables.

Article 35.

Le fournisseur de services numériques a l'obligation de garantir l'accès aux services d'urgence conformément aux règles applicables et dans les conditions précisées par l'Autorité de Régulation du Numérique.

L'accès à ces services dans les zones couvertes par les activités du fournisseur ne peut souffrir d'aucune limitation.

Article 36.

Le fournisseur de services numériques ne peut utiliser leurs infrastructures ou sciemment en permettre l'utilisation à des fins contraires aux dispositions légales et réglementaires en vigueur.

Il est tenu de prendre toutes mesures appropriées pour s'assurer que ses infrastructures ne soient pas utilisées à des fins illégales ou frauduleuses.

Article 37.

Sauf en cas de réquisitions judiciaires, le fournisseur de services numériques est tenu aux exigences de confidentialité des données qu'il traite conformément aux dispositions du Livre III de la présente ordonnance-loi.

TITRE V : DE L'ADMINISTRATION DÉMATÉRIALISÉE

CHAPITRE I : DES ECHANGES D'INFORMATION AU SEIN DE L'ADMINISTRATION PUBLIQUE

Article 38.

L'administration publique répond par voie électronique à toute demande d'information qui lui est adressée que ce soit par une personne ou par une autre administration.

L'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.

À ce titre, 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 39.

Les administrations échangent par voie électronique entre elles toutes les informations ou données strictement nécessaires pour traiter une requête.

Le gouvernement met en place une infrastructure informatique sécurisée de transmission d'informations entre les différentes administrations publiques au niveau central et provincial sous forme d'un intranet gouvernemental ou provincial.

Article 40.

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 du Ministre ayant le numérique dans ses attributions en fixe les modalités de mise en œuvre.

CHAPITRE II : DU GUICHET NUMERIQUE

Article 41.

Le Gouvernement met en place un système intégré d'échanges et d'activités électroniques, de fourniture des services, de prestations étatiques et autres interventions de l'État dans les réseaux locaux et distants, dénommé « Guichet Numérique de la République Démocratique du Congo », en sigle GN-RDC.

Le GN-RDC est placé sous l'autorité et le contrôle du Ministre ayant le numérique dans ses attributions.

Un Décret du Premier Ministre fixe l'organisation du GN-RDC sur proposition du Ministre ayant le Numérique dans ses attributions.

TITRE VI : DE L'ARCHIVAGE ÉLECTRONIQUE

CHAPITRE I : DISPOSITIONS GENERALES

Article 42.

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 ;
2. Le document est conservé en 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 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 conservées par ce moyen.

Article 43.

Les données concernées par l'archivage électronique doivent être structurées, indexées et conservées sur des formats appropriés à la conservation et à la migration.

L'archivage électronique garantit, dans leur intégrité, la restitution des données conservées ou leur accessibilité dans un contexte technologique changeant.

Les règles de l'archivage électronique s'appliquent indifféremment aux documents numérisés et aux documents conçus initialement sur support électronique.

Article 44.

Un Décret du Premier Ministre, sur proposition des Ministres ayant respectivement le numérique et la culture dans leurs attributions, fixe les conditions et les modalités de l'archivage électronique.

CHAPITRE II : DES ARCHIVES NUMERIQUES PUBLIQUES

Article 45.

L'Institut National des Archives du Congo, désigné par le 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 46.

Aux fins du financement de l'archivage des archives numériques publiques par l'Institut National des Archives du Congo, une redevance est instituée sur tous les actes et documents émis par les services et établissements publics et destinés à être sauvegardés ou archivés. La redevance pour archivage est une quotité appliquée sur le prix de l'obtention desdits actes ou documents.

Un arrêté interministériel des Ministres ayant respectivement les Finances, le numérique et la culture et patrimoine, dans leurs attributions fixe le taux, la liste des actes et documents, ainsi que les mécanismes de perception, de recouvrement et de rétrocession à l'Institut National des Archives du Congo de la redevance évoquée à l'alinéa précédent.

TITRE VII : DES DROITS DE LA PROPRIETE INTELLECTUELLE ET INDUSTRIELLE

CHAPITRE I : DISPOSITIONS GENERALES

Article 47.

Constituent aussi les œuvres de l'esprit protégées respectivement par la loi n° 82-001 du 7 janvier 1982 sur la propriété industrielle et l'ordonnance-loi n° 86-033 du 5 avril 1986 portant protection des droits d'auteurs et des droits voisins en République Démocratique du Congo, notamment : les logiciels, les applications, les plateformes numériques, y compris le matériel de conception préparatoire.

Un Décret du Premier Ministre délibéré en Conseil des ministres, sur proposition des Ministres ayant le numérique et l'industrie dans leurs attributions, précise les droits et détermine les critères, les conditions et modalités d'octroi, le cas échéant, de retrait des titres qui consacrent les droits visés à l'alinéa précédent.

TITRE VIII : DU COMMERCE ÉLECTRONIQUE

CHAPITRE I : DISPOSITIONS GENERALES

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

Article 48.

Le présent titre fixe les règles générales régissant les échanges et les transactions 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 aux places de marché numériques « marketplace ».

Sans préjudice des dispositions de la loi n° 01-10-19 du 09 Juillet 2018 relative aux systèmes de paiement et de règlement-titres, il s'applique également aux établissements de crédit, aux institutions de microfinance ainsi qu'aux services financiers intervenant par voie électronique.

Section 2 : Des principes régissant le commerce électronique

Article 49.

Le commerce électronique est soumis aux principes suivants :

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

Article 50.

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, à la protection des personnes ou de l'environnement, 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 ordonnance-loi ou aux dispositions légales et réglementaires en vigueur.

Un arrêté interministériel des Ministres en charge du commerce et le numérique détermine les modalités d'application des restrictions mentionnées à la ligne précédente.

Article 51.

La personne physique ou morale exerçant les échanges électroniques et transactions électroniques est responsable de plein droit à l'égard de son co-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 de services, sans préjudice de son droit de recours contre ceux-ci.

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

Article 52.

Sans préjudice 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 pour les 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 Registre de Commerce et du Crédit Mobilier, sa forme juridique, son 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 prévues par les dispositions légales et réglementaires en vigueur.

CHAPITRE II : DE LA CONCLUSION DU CONTRAT SOUS FORME ELECTRONIQUE

Section 1 : Principe et contenu de l'offre

Article 53.

Toute personne qui 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 à 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 54.

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 55.

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 55 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 : Responsabilité contractuelle des parties

Article 56.

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 transmise au client.

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

CHAPITRE III : DE L'EXECUTION DU CONTRAT ELECTRONIQUE

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

Article 57.

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

Article 58.

À la livraison effective du produit ou à la fourniture du service objet du contrat électronique, le fournisseur exige du client d'en accuser réception et le client est tenu de s'exécuter.

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 livraison, ou lorsque les conditions de l'offre ne sont pas remplies, le client peut réexpédier le produit dans un délai n'excédant pas quatre (04) 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 (15) jours à compter de la date de réception du produit.

Article 59.

En cas de livraison d'un article non conforme à la commande ou dans le cas d'un produit défectueux, le fournisseur reprend sa marchandise.

Lorsque le produit défectueux constitue une menace à la santé publique, à la sécurité ou à l'environnement, celui-ci est constaté et détruit par les services compétents conformément à la législation en vigueur.

Le client réexpédie la marchandise dans son emballage d'origine dans un délai maximal de sept (07) jours augmentés du 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.

À défaut pour le client de réexpédier la marchandise dans le délai prévu à l'alinéa précédent, 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 (15) jours à compter de la date de réception du produit.

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

Article 60.

Le 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 trouvant 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 IV : DU DROIT DE RETRACTATION

Article 61.

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

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

Section 1 : Délai de rétractation

Article 62.

Nonobstant l'accord entre les parties, avant le jour de l'expédition prévu dans le contrat, le client dispose d'un délai de soixante-douze (72) heures pour exercer son droit de rétractation.

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

Dans le cas où les informations prévues aux articles 49 et 52 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 (48) heures au plus de la passation de la commande, s'agissant des contrats portant sur la fourniture de services.

Dans le cas où le professionnel manque à son obligation d'information préalable prévue à l'article 49 du présent Livre, le délai de rétractation est porté à quinze (15) jours.

Le client notifie au professionnel sa décision d'exercer son droit de rétractation par courrier électronique dans le délai de soixante-douze (72) heures prévues à l'alinéa 1 ci-dessus.

Section 2 : Droits et obligations du professionnel

Article 63.

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 (72) heures, à compter de la date de réception de la notification de la rétractation.

En cas de non-remboursement 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 64.

Le client perd son droit de rétractation, lorsque :

1. Le bien a été livré et réceptionné par le client conformément à la commande;
2. Le service a été fourni;
3. 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 65.

Nonobstant l'accord 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 (02) 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 (72) 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 (05) jours ouvrables à compter du jour de la notification de la résiliation par le client.

CHAPITRE V : DE LA PUBLICITE PAR VOIE ELECTRONIQUE

Section 1 : Des dispositions générales

Article 66.

Sans préjudice des dispositions légales applicables en matière de publicité en République Démocratique du Congo, toute publicité, sous quelque forme que ce soit, accessible par un service de communications électroniques ouvert au public ou un service en ligne, doit 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, en portant à la connaissance des destinataires des services son nom, son adresse géographique à laquelle elle est établie, ses coordonnées y compris son adresse courrier électronique, éventuellement son Registre de Commerce et de Crédit Mobilier, son numéro d'impôt, et l'acte juridique qui autorise l'exercice de l'activité.

La publicité peut notamment être identifiée comme telle en raison de son titre, de sa présentation ou de son objet.

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

Article 67.

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, sont identifiables comme telles dès réception par l'utilisateur ou dès que ce dernier y a accès.

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

De même, les concours ou jeux promotionnels sont 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 sont 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.

Section 2 : Des conditions de la prospection directe

Article 68.

Est interdite la prospection directe au moyen de systèmes automatisés de communications électroniques, de réseaux, de services et/ou de terminaux de communications électroniques, de télécopieurs, de courriers électroniques et de 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.

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 69.

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 ordonnance-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 70.

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 71.

Lorsque la prospection directe est destinée aux enfants, aux personnes âgées, aux personnes malades ou vulnérables, ou à toute personne qui n'est pas en mesure de comprendre pleinement les informations qui lui sont présentées, les exceptions prévues au présent Titre doivent être interprétées plus strictement et sans dol.

Article 72.

Il est interdit d'émettre, à des fins de prospection directe, des messages au moyen de systèmes automatisés de communications électroniques, de réseaux, de services et/ou de terminaux de communications électroniques, télécopieurs, de courriers électroniques ou de SMS, sans indiquer les moyens et les coordonnées valables auxquels le destinataire transmet 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 III de la présente ordonnance-loi 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.

À cette fin, elle recueille notamment, par tous moyens, les plaintes concernant les manquements aux dispositions du présent article.

TITRE VIII : DES PLATEFORMES NUMÉRIQUES ET DES FOURNISSEURS EN POSITION DOMINANTE

Article 73.

La position dominante concerne notamment les fournisseurs d'accès internet, les services informatiques en nuage, les places de marché, les boutiques d'applications, les réseaux sociaux, les

plateformes de partage de contenus, les plateformes de banque en ligne, les technologies financières, de voyage, de transport, d'hébergement et les moteurs de recherche.

La position dominante du fournisseur des activités et services numériques est appréciée sur la base des critères suivants :

1. sa capacité à influencer le marché ;
2. son chiffre d'affaires par rapport à 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 74.

Un arrêté du Ministre ayant le numérique dans ses attributions fixe les modalités d'application des dispositions relatives à la régulation des plateformes numériques et fournisseurs en position dominante, l'Autorité de Régulation du Numérique étant entendue par un avis conforme.

TITRE IX : DE LA SURVEILLANCE, DU CONTRÔLE TECHNIQUE DES ACTIVITÉS ET SERVICES NUMÉRIQUES, DU RÈGLEMENT DES DIFFÉRENDS, DES MESURES ET SANCTIONS ADMINISTRATIVES ET DE LA PRESCRIPTION

CHAPITRE I : DE LA SURVEILLANCE ET DU CONTROLE TECHNIQUE DES ACTIVITES ET SERVICES NUMERIQUES

Article 75.

La surveillance du secteur du numérique est assurée par le Ministre ayant le numérique dans ses attributions et, le cas échéant, à travers les établissements, services et/ou organismes y rattachés conformément aux dispositions de la présente ordonnance-loi ainsi qu'aux lois et règlements en vigueur.

Le fournisseur des activités et services numériques a l'obligation de coopérer et d'agir promptement à la suite d'une violation signalée par les organes repris à l'article précédent, sur demande de ces derniers. Un arrêté du Ministre chargé du numérique fixe les conditions et modalités de surveillance et de contrôle technique des activités et services numériques.

CHAPITRE II : REGLEMENT DES DIFFERENTS

Article 76.

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

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

Article 77.

L'Autorité de Régulation du Numérique 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.

À ce titre, elle saisit l'Autorité de Régulation du Numérique du pays du fournisseur des activités et services numériques mis en cause.

Article 78.

Lorsque l'Autorité de Régulation du Numérique 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 du Numérique coordonne ses efforts avec elle dans le règlement du différend.

Article 79.

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

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

Article 80.

L'Autorité de Régulation du Numérique procède à une tentative de règlement amiable en cas de contentieux entre fournisseurs de services numériques ou entre ces derniers et les utilisateurs.

Elle instruit les demandes dans un délai qui ne peut dépasser trente (30) jours ouvrables à dater de sa saisine.

Les décisions de l'Autorité de Régulation du Numérique sont motivées et sont susceptibles d'un recours juridictionnel devant le Conseil d'État 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.

CHAPITRE II : DES MESURES ET SANCTIONS ADMINISTRATIVES

Article 81.

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 dispositions de la présente ordonnance-loi ainsi que des ses mesures réglementaires applicables, y compris celles de son cahier de charges, sur proposition ou après avis émanant de l'Autorité de Régulation du Numérique ou de l'Autorité Nationale de Certification Électronique, le Ministre ayant le numérique dans ses attributions le met en demeure de s'y conformer dans un délai de quinze (15) 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. au paiement d'une amende ;
2. la réduction de la durée de validité du titre ;
3. la suspension du titre ;
4. au retrait du titre.

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

CHAPITRE III : DE LA PRESCRIPTION

Article 82.

1. La prescription est acquise :
2. Au profit des fournisseurs de services numériques dans leurs relations contractuelles avec les utilisateurs, pour toute demande de restitution du prix de leurs prestations présentée par un utilisateur après un délai de 365 jours à compter de la date du paiement ;
3. Au profit des utilisateurs dans leurs relations contractuelles avec les fournisseurs de services numériques, pour les sommes dues à un fournisseur de services numériques au titre du paiement de ses prestations, lorsque celui-ci ne les a pas réclamées dans un délai de 365 jours à compter de la date de leur exigibilité.

LIVRE II : DES ÉCRITS, DES OUTILS ÉLECTRONIQUES ET DES PRESTATAIRES DE SERVICES DE CONFIANCE

TITRE I : DES ÉCRITS ET OUTILS ÉLECTRONIQUES

CHAPITRE I : DES DISPOSITIONS GENERALES

Article 83.

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

Il fixe les règles et principes applicables notamment à :

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

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

CHAPITRE II : DE L'ECRIT ELECTRONIQUE

Section 1 : Des principes généraux

Article 84.

L'écrit électronique obéit aux principes de :

1. intégrité ;
2. liberté ;
3. transparence ;
4. clarté.

Article 85.

L'intégrité d'un écrit électronique résulte de :

1. La possibilité de vérifier que l'information n'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 86.

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

Article 87.

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 88.

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

Section 2 : Validité de l'écrite électronique

Article 89.

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

Article 90.

L'acte authentique établi sur support électronique a la même valeur juridique que l'acte authentique sur papier sous réserve des conditions de validité prévues dans la présente ordonnance-loi.

Un arrêté interministériel des Ministres ayant respectivement la justice et le numérique dans leurs attributions, définit les conditions et modalités du présent article.

Article 91.

L'écrit électronique est horodaté et comporte une signature électronique certifiée.

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

Article 92.

Sous réserve de dispositions légales particulières, lorsqu'un écrit est exigé pour la validité d'un acte juridique, il est 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, prennent la forme d'écrit électronique à condition qu'il respecte, en plus de ces exigences particulières, celles du présent Livre.

Article 93.

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

1. les contrats ;
2. les actes relatifs au droit civil des personnes ;
3. les actes relatifs aux sûretés personnelles ou réelles, de nature civile ou commerciale ;
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. les actes déclaratifs et liquidatifs des administrations fiscales, parafiscales, douanières et de sécurité sociale ;
7. les factures des biens, prestations diverses des personnes physiques ou morales, publiques ou privées ;

8. 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.

Article 94.

Les professions juridiques et judiciaires recourent aux écrits et outils électroniques dans l'établissement de leurs actes et dans l'administration de la preuve.

Les acteurs de ces professions, notamment les notaires et les huissiers de justice, garantissent la sécurité juridique et technique par des procédés de vérification et de certification.

L'ensemble des informations concernant l'acte, dès son établissement, telles que les données permettant de l'identifier, de déterminer ses propriétés et d'en assurer la traçabilité, est également conservé.

Section 3 : De la preuve électronique

Article 95.

L'écrit 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 en garantir l'intégrité conformément à la législation relative à la conservation des archives.

Article 96.

La conservation des écrits sous forme de 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 ;
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 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 Nationale de Certification Électronique.

Article 97.

Tout document, enregistrement, contenu ou information électronique satisfait aux obligations légales de présenter ou conserver les informations qu'ils contiennent sous leur forme originale, dès lors que :

- l'intégrité et l'exactitude des informations générées sont garanties et maintenues de manière fiable ;
- 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 98.

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 originel.

L'intégrité est prouvée au moyen d'un certificat de conformité délivré par un prestataire de services de confiance conformément au Livre II de la présente ordonnance-loi.

Article 99.

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

Cette certification est fournie par un prestataire de services de confiance conformément aux dispositions du Livre II de la présente ordonnance-loi.

Article 100.

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

Article 101.

La 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 102.

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.

Elles bénéficient également d'une présomption de l'exactitude de la date et de l'heure d'envoi et de réception, lors de leur réception par le destinataire identifié par le service d'envoi électronique recommandé qualifié.

Article 103.

Les services d'envoi recommandé électronique qualifié doivent :

1. être fournis par un ou plusieurs prestataires de services de confiance qualifiés ;
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 certifié.

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

CHAPITRE III : DES OUTILS ELECTRONIQUES

Section 1 : De la signature électronique

Article 104.

Sans préjudice des dispositions légales particulières en vigueur en République Démocratique du Congo, 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. La signature électronique est admise dans les échanges et les transactions électroniques.

La signature électronique peut être simple ou qualifiée.

Article 105.

Toute personne désireuse d'apposer sa signature électronique simple sur un document recourt au prestataire des services de confiance.

Article 106.

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 107.

La fiabilité d'un procédé de signature électronique est présumée établie jusqu'à preuve du contraire lorsque ce procédé met en œuvre une signature électronique qualifiée ; et ce, 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 108.

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

Article 109.

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

Article 110.

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.

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

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

Article 111.

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 la base de fausses informations ;
2. le certificat a été délivré sur la base d'une cause ou d'un objet illicite ;
3. le certificat a été délivré en violation des dispositions de la présent ordonnance-loi.

Article 112.

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 des 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 des données de création de signature électronique pour le compte du signataire est exclusivement confiée à un prestataire de services de confiance qualifié.

Article 113.

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 114.

La certification du dispositif de création de signature électronique simple ou qualifiée est assurée par l'Autorité Nationale de Certification Électronique suivant les exigences techniques fondamentales d'après :

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.

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 115.

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

1. la conformité du certificat aux exigences du présent texte ;
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 à valider 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 y a lieu ;
6. la certitude qu'elle est créée par un dispositif de création qualifié et certifiée.

Article 116.

Les services de validation qualifiés 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 qualifiée ou le cachet électronique qualifié du prestataire qui fournit le service de validation qualifié.

Article 117.

Le 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.

Section 2 : Du cachet électronique

Article 118.

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 119.

Les dispositions de l'article 106 s'appliquent mutatis mutandis aux exigences du cachet électronique qualifié.

Article 120.

Sans préjudice des dispositions de la présente ordonnance-loi, 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 à la présente ordonnance-loi.

Article 121.

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

1. Ceux qui reposent sur un certificat qualifié ;
2. Ceux dont les formats utilisent 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 cachets électroniques dans le secteur public.

Article 122.

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 sociale 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 123.

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 124.

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

Section 3 : De l'horodatage électronique

Article 125.

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 certifié.

Un horodatage électronique certifié 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 126.

L'horodatage électronique certifié satisfait aux exigences suivantes :

1. Lier la date et l'heure aux données de manière à exclure la possibilité d'une modification indéfectible 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 cacheté au moyen d'un cachet électronique qualifié du prestataire de services de confiance qualifié.

Section 4 : De l'authentification de sites internet

Article 127.

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 post-nom ;
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 sociale 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) exploités 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 repose la signature électronique qualifiée ou le cachet électronique qualifié visé 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 128.

Le certificat qualifié d'authentification de site internet est délivré par un prestataire de services de confiance qualité et satisfait aux exigences prévues à l'article 127 de la présente ordonnance-loi.

TITRE II : DES PRESTATAIRES DE SERVICES DE CONFIANCE

CHAPITRE I : DES DISPOSITIONS GENERALES

Article 129.

Les dispositions légales relatives aux services de confiance s'appliquent aux prestataires de services de confiance établis ou à destination de la République Démocratique du Congo.

Elles fixent :

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 sites Internet.

Article 130.

Sont considérés comme prestataires de services de confiance, les fournisseurs des services suivants :

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

8. la cryptologie.

Un arrêté du Ministre ayant le Numérique dans ses attributions complète la liste des prestataires des services de confiance, l'Autorité Nationale de Certification Électronique entendue par avis écrit.

Article 131.

Sur proposition du Ministre ayant le Numérique dans ses attributions, le Gouvernement met en place une infrastructure à clés publiques nationale, socle des techniques des services de confiance, et détermine les modalités de sa mise en œuvre et de son exploitation.

CHAPITRE II : PRINCIPES ET CATEGORIES DES PRESTATAIRES

Section 1 : Des principes

Article 132.

Les prestataires de services de confiance obéissent aux principes de :

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

Article 133.

Le prestataire de services 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 134.

Le prestataire de services de confiance qui fournit un ou plusieurs services est libre d'utiliser toute technologie, certifiée par l'Autorité Nationale de Certification Electronique, qui garantit l'inviolabilité de plusieurs services de confiance fournis.

Article 135.

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 les deux conditions suivantes sont remplies :

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 Nationale de Certification Electronique.

Section 2 : Des catégories de prestataires de services de confiance

Article 136.

Les prestataires de services de confiance sont de deux catégories :

1. les prestataires de services de confiance qualifiés ;
2. les prestataires de services de confiance non qualifiés.

Article 137.

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

Article 138.

L'autorisation et la déclaration s'effectuent conformément aux dispositions du Livre premier de la présente ordonnance-loi.

Article 139.

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 de la présente ordonnance-loi.

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 140.

Les prestataires de services de confiance non-qualifiés qui souhaitent exercer des services de confiance qualifiés soumettent à l'Autorité Nationale de Certification Electronique, une demande accompagnée d'un rapport d'évaluation de conformité.

Article 141.

L'Autorité Nationale de Certification Electronique vérifie notamment que les demandes des prestataires de services de confiance et les services de confiance fournis sont conformes aux dispositions de la présente ordonnance-loi.

L'Autorité Nationale de Certification Electronique statue dans un délai de trente (30) jours à dater de la demande.

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

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

Article 142.

L'admission des prestataires de services de confiance à l'un des régimes juridiques prévus par la présente ordonnance-loi tient compte de ou des :

1. l'infrastructures, des mesures techniques de sécurité et d'organisation mises en place par le prestataire ;
2. la régularité et 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.

CHAPITRE III : OBLIGATIONS ET RESPONSABILITES

Section 1 : Des obligations et responsabilité des prestataires de service de confiance

Paragraphe 1 : Des obligations

Article 143.

Le prestataire de services de confiance qualifié établi en République démocratique du Congo est tenu de soumettre à l'Autorité Nationale de Certification Électronique, notamment, les informations suivantes :

1. Pour une personne physique :
   - ses prénoms, 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 Registre de Commerce et du Crédit Mobilier ;
   - sa dénomination sociale ;
   - 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 144.

Le prestataire de services de confiance qualifié doit :

1. informer l'Autorité Nationale 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 qualifiée 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 déterminée 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 informatiques ;

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 de la présente ordonnance-loi ;
15. établir, rendre public 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 145.

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 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 146.

Sans préjudice des dispositions du Livre III de la présente ordonnance-loi, 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 à sa disposition.

Article 147.

Les prestataires de services de confiance qualifiés et non-qualifiés sont tenus de prendre les mesures techniques et organisationnelles nécessaires afin de prévenir et de 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 proportionnel au degré de risques.

Des mesures sont notamment prises en vue de prévenir et de 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 148.

Les prestataires de services de confiance qualifiés et non-qualifiés notifient à l'Autorité Nationale de Certification Électronique par tout moyen, et le cas échéant, aux autres organismes concernés, dans un délai de vingt-quatre (24) heures après en avoir eu connaissance, toute atteinte à la sécurité ou toute perte d'intégrité ayant une incidence significative sur le service de confiance fourni ou sur les données à caractère personnel qui y sont conservées.

Article 149.

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 également l'atteinte à la sécurité ou la perte d'intégrité dans un délai de vingt-quatre (24) heures.

Lorsque l'atteinte à la sécurité ou la perte d'intégrité concerne un État étranger, l'Autorité Nationale de Certification Électronique qui en a reçu la notification en informe préalablement les autorités compétentes.

L'Autorité Nationale de Certification Électronique informe par ailleurs le public ou exigé du prestataire de services de confiance qu'il informe le public, dès lors que l'Autorité Nationale 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 150.

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 incluent 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 Nationale de Certification Électronique.

Article 151.

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

Article 152.

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

1. il existe des raisons sérieuses indiquant 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 violées ou risque de l'être ;
2. le prestataire de services de confiance prend les mesures nécessaires pour répondre à tout moment et sans délai à une demande de révocation.

Article 153.

Lorsque la décision de révocation est prise, le prestataire de services de confiance notifie la révocation du certificat au titulaire dans un délai de trente (30) 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.

Paragraphe 2 : De la responsabilité

Article 154.

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 Nationale de Certification Électronique, il ne peut être tenu responsable des dommages survenus par l'utilisation des services au-delà de ses limites.

Section 2 : Obligation et responsabilité du titulaire du certificat

Paragraphe 1 : De l'obligation

Article 155.

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 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.

Paragraphe 2 : De la responsabilité

Article 156.

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

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

TITRE V : DU CONTRÔLE DES PRESTATAIRES DE SERVICES DE CONFIANCE

Article 157.

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

Article 158.

Les prestataires de services de confiance qualifiés font l'objet, tous les vingt-quatre (24) mois, d'un audit effectué par un cabinet d'audit ou un organisme d'évaluation de la conformité.

L'objectif 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 la présente ordonnance-loi.

Dans un délai de dix (10) jours ouvrables suivant sa réception, les prestataires de services de confiance qualifiés transmettent le rapport d'évaluation de conformité à l'Autorité Nationale de Certification Electronique.

Article 159.

Sans préjudice des dispositions de l'article précédent, l'Autorité Nationale de Certification Electronique 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 de conformité réalisés par l'Autorité Nationale de Certification Electronique 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 elle dispose.

Article 160.

L'Autorité Nationale de Certification Electronique 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 Nationale de Certification Electronique établit, tient à jour et publie de façon sécurisée et sous une forme adaptée au traitement automatisé, les listes de confiances visées à l'article 1 relatives aux signatures électroniques et aux cachets électroniques.

L'Autorité Nationale de Certification Electronique 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 ACTIVITÉS

Article 161.

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 volontairement de quitter le secteur ;
4. s'il est sujet à une sanction administrative.

Article 162.

Le prestataire de services de confiance informe l'Autorité Nationale de Certification Électronique soixante (60) 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 équivalent. Ce transfert d'activités est réalisé sous le contrôle de l'Autorité Nationale de Certification Électronique.

En l'absence de repreneur, le prestataire révoque, sous réserve d'un préavis de soixante (60) jours, les certificats octroyés à ses titulaires.

Article 163.

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 Nationale de Certification Électronique. Il procède, le cas échéant, à la révocation des certificats délivrés.

TITRE VII : DES SANCTIONS ADMINISTRATIVES

Article 164.

Lorsque le prestataire de services de confiance ne se conforme pas aux dispositions de la présente ordonnance-loi et aux exigences fixées par l'Autorité Nationale de Certification Électronique, cette dernière prononce à son encontre, dans le respect du principe du contradictoire, les sanctions suivantes :

1. l'injonction de cesser pour une durée de nonante (90) à trois cent soixante-cinq (365) jours 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 pour le prestataire de services de confiance d'informer immédiatement les titulaires des certificats qualifiés qu'il a délivrés, de leur non-conformité aux dispositions de la présente ordonnance-loi 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 sûreté de l'État.

Article 165.

Lorsque l'Autorité Nationale de Certification Électronique exige du prestataire de services de confiance qualifié qu'il corrige un manquement aux exigences prévues dans la présente ordonnance-loi 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.

L'Autorité Nationale 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.

Le prestataire de services de confiance dispose, préalablement à tout recours juridictionnel, d'un droit de recours gracieux auprès de l'Autorité de certification.

Le recours juridictionnel est exercé devant la Cour d'appel conformément à la loi organique n° 16-027 du 18 octobre 2016 portant organisation, compétence et fonctionnement des juridictions de l'ordre administratif.

LIVRE III : DES CONTENUS NUMERIQUES

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

Article 166.

Sans préjudice des dispositions légales et réglementaires particulières, le présent Livre fixe les règles relatives aux données publiques et à la protection des données à caractère personnel.

TITRE II : DES CONTENUS PUBLICS

CHAPITRE I : DISPOSITIONS GENERALES

Article 167.

Les données publiques sont celles produites, reçues ou traitées dans le cadre des missions de service public par l'administration, l'établissement, l'organisme et l'entreprise publics ou les personnes morales de droit privé chargée d'une telle mission et sont stockées dans les registres publics de données de la République Démocratique du Congo.

Article 168.

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

1. **Registre National de la Population** : registre d'identité, registre de l'état civil, registre biométrique.
2. **Registre de terrains et propriétés** : registre cadastral, registre de propriété, registre des actes notariés immobiliers, registre des baux, registre des mines, registre forestier, registre agricole.
3. **Registre de permis et licences** : registre des concessions, registre des licences commerciales et/ou permis, registre personnel des licences et/ou permis, registre des permis de conduire.
4. **Registre des factures et paiements** : registre des factures, registre des points de vente, registre du commerce électronique et registre des paiements électroniques.
5. **Registre des citoyens et des migrants** : registre des personnes physiques, registre des bénéficiaires effectifs, et registre des visas.
6. **Registre des actifs** : registre des véhicules automobiles, registre téléphonique, registre des aéroports.
7. **Registre judiciaire** : registre des décisions prises par les Cours et tribunaux de tous les ordres de juridiction.
8. **Registre de la santé, de l'éducation, des activités sociales**, etc.

Conformément aux dispositions de la présente ordonnance-loi, les 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.

Un Décret du Premier Ministre délibéré en Conseil des Ministres et complète, sur proposition du Ministre ayant le numérique dans ses attributions en collaboration avec les Ministres sectoriels concernés, la liste et les catégories des registres publics de données mentionnées dans le présent article, l'Autorité de Données Personnelles étant consultée par avis écrit.

Article 169.

Les administrations sont tenues de publier en ligne et/ou de communiquer les documents administratifs qu'elles détiennent aux personnes qui en font la demande dans les conditions prévues par la présente ordonnance-loi.

Article 170.

Le droit à la communication ne s'applique qu'aux documents finaux.

Ce droit à la communication ne concerne pas :

- les documents préparatoires à une décision administrative tant qu'elle est en cours d'élaboration ;
- les documents qualifiés de stratégiques par l'État ;
- les documents relevant de la vie privée ;
- les documents liés à la défense et à la sécurité nationale ;
- les documents dont les tiers détiennent les droits de propriété.

Un arrêté du Ministre ayant le numérique dans ses attributions complète ou modifie la liste des documents qui ne sont pas soumis au droit à la communication selon les circonstances par voie réglementaire.

CHAPITRE II : DE L'IDENTIFICATION ELECTRONIQUE

Section 1 : Des principes et des obligations

Article 171.

L'identification électronique est un processus qui consiste à l'utilisation des données d'identité d'une personne physique ou morale par des procédés électroniques qui représentent de manière univoque la personne physique ou morale concernée.

Article 172.

L'État procède, au moyen d'identification électronique, à l'identification générale de la population et délivre une carte d'identité nationale à l'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 173.

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 éléments, les spécifications techniques des moyens d'identification électronique, les schémas d'identification électronique et leurs niveaux de garantie certifiant l'identification ainsi que le cadre d'interopérabilité.

Section 3 : Schéma électronique

Article 174.

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 :

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 ;

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 ;

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 175.

Le 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 prévus à l'article 174 ;
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 176.

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 175 de la présente ordonnance-loi.

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 177.

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 Nationale de Certification Electronique 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 178.

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 conformément à la législation en vigueur.

Article 179.

Les schémas d'identification électronique sont interopérables.

Article 180.

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 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 de la présente ordonnance-loi.

Article 181.

La fixation du cadre d'interopérabilité répond aux exigences :

1. d'une référence aux exigences techniques minimales liées aux niveaux de garantie prévus à l'article 174 ;
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 174 ;
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 4 : Obligations liées au moyen d'identification électronique

Article 182.

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 l'échéance ou est révoqué, son titulaire ne peut plus l'utiliser.

TITRE III : DES DONNÉES PERSONNELLES

CHAPITRE I : DISPOSITIONS GENERALES

Article 183.

Les catégories suivantes sont considérées comme données personnelles. Il s'agit notamment de :

1. des données d'identification personnelle notamment : prénom, nom, post-nom, date et lieu de naissance, âge, état civil, numéro d'identification nationale, document officiel d'identité en cours de validité et 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 les données personnelles ;
7. des données sur la situation familiale ;
8. des données concernant des décisions de justice.

Article 184.

Sont soumis aux dispositions du présent Titre :

1. la collecte, le traitement, la transmission, le stockage et l'utilisation des données à caractère personnel par l'État, la Province, les Entités Territoriales Décentralisées et Déconcentrées, les personnes morales de droit public ou de droit privé et les personnes physiques,
2. le traitement automatisé ou non de données contenues ou appelées à figurer dans un fichier ;
3. le traitement de données mis en œuvre sur le territoire national ou à l'étranger ;
4. le traitement de données concernant la sécurité publique, la défense, la recherche et la poursuite d'infractions pénales ou la sûreté de l'État, sous réserve des dérogations définies par des dispositions spécifiques fixées par d'autres textes de loi en vigueur.

Article 185.

Sont exclus du champ d'application du présent titre :

1. le traitement des 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 informatique, en vue du stockage automatique, intermédiaire et transitoire des données et à la seule fin de permettre à d'autres destinataires du service le meilleur accès possible aux informations transmises ;

3. les traitements des données à caractère personnel effectués par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution des sanctions pénales, y compris la protection contre des menaces ou la sécurité publique et la prévention de telles menaces.

CHAPITRE II : CONDITIONS DE TRAITEMENT DES DONNEES PERSONNELLES

Article 186.

Le traitement des données personnelles 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 présente ordonnance-loi.

L'Autorité de protection des données délivre un récépissé en réponse à la déclaration, le cas échéant par voie électronique. Le demandeur met 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 187.

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 même nature, notamment les numéros de téléphone ;

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 188.

Les demandes de déclaration et d'autorisation contiennent :

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 service(s) chargé(s) de mettre en œuvre le traitement ainsi que les catégories de personnes qui, en raison de leurs fonctions ou pour les besoins du service, ont directement accès aux données enregistrées ;
6. les destinataires ou catégories de destinataires habilités à recevoir la 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 entourent 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 titre.

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

Article 189.

Sont dispensés des formalités de déclaration préalable :

1. le traitement de données utilisées par une personne physique dans le cadre exclusif de ses activités personnelles, domestiques ou familiales ;
2. le traitement de données concernant une personne physique dont la publication est prescrite par une disposition légale ou réglementaire ;
3. le traitement de données ayant pour seul objet la tenue d'un registre qui est destiné à un usage exclusivement privé ;
4. 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 titre, sauf lorsqu'un transfert de données à caractère personnel à destination d'un pays tiers est envisagé ;
5. le traitement des données à caractère personnel mis en œuvre par les organismes et entreprises publics ou privés pour la tenue de leur comptabilité générale ;
6. le traitement des données personnelles mis en œuvre par les organismes et entreprises publics ou privés relatifs à la gestion des rémunérations de leur personnel ;

7. le traitement des données personnelles mis en œuvre par les organismes publics ou privés pour la gestion de leurs fournisseurs ;
8. le traitement 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 190.

L'Autorité de protection des données se prononce dans un délai de trente (30) jours à compter de la réception de la demande de déclaration ou d'autorisation.

Toutefois, ce délai peut être prorogé une fois, de trente (30) 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 rendue dans le délai prévu, le silence de l'Autorité de protection des données vaut acceptation.

En cas de refus de l'Autorité de protection des données, il est accordé au responsable du traitement le droit de recours gracieux dans un délai de quinze jours à partir de la notification de la décision du refus.

Article 191.

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

CHAPITRE III : DU TRAITEMENT DES DONNEES PERSONNELLES

Article 192.

Le traitement des données personnelles n'est licite que dans la mesure où la personne concernée a consenti au traitement de ses données à caractère personnel ou si le traitement est nécessaire à l'exécution d'une obligation légale à laquelle le responsable du traitement est soumis.

Le traitement de données personnelles se fait dans le cadre du respect de la dignité humaine, de la vie privée et des libertés publiques.

Le traitement des données personnelles, 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 à leur réputation.

Article 193.

Les données personnelles sont :

1. traitées de manière licite, loyale et transparente :
   - la personne concernée donne 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 des 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 personnelles 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 titre afin de garantir les droits et libertés de la personne concernée sous réserve des dispositions de la Loi n°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 194.

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

Toutes les mesures appropriées 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 195.

Est interdit de traitement des données à caractère personnel ayant trait aux informations raciales, ethniques, aux opinions politiques, aux convictions religieuses ou philosophiques, aux statuts de réfugiés 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 ses 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 nécessaire à l'exécution d'une mission d'intérêt public ou 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 effectué en exécution de lois relatives aux statistiques publiques ;

7. Le traitement nécessaire aux fins de médecine préventive ou de 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 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 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 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 nécessaire au respect d'une obligation légale ou réglementaire à laquelle le responsable du traitement est soumis ;

12. Le traitement nécessaire afin d'exécuter les obligations et les droits spécifiques du responsable du traitement en matière de droit du travail ;

13. Le traitement 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 papier, un support électronique ou tout autre support équivalent ;

14. Le traitement 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 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 font 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 aux droits en vigueur en République Démocratique du Congo ou aux règles arrêtées par les organismes nationaux compétents.

Article 196.

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.

Au cas où 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 IV : DE LA TRANSMISSION ET DU TRANSFERT DES DONNEES PERSONNELLES

Section 1 : De la transmission des données personnelles

Article 197.

La transmission de données personnelles est licite et légale. Elle se fait entre les responsables de traitement de droit privé et/ou de droit public.

Article 198.

Le responsable de traitement transmet à un ou plusieurs autres responsables de traitement des données personnelles pour des besoins 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.

Un accord de confidentialité est conclu entre les deux responsables de traitement.

Article 199.

Pour des raisons d'enquête judiciaire, le Ministère public ou le juge adresse une réquisition d'information ou une requête au responsable de traitement aux fins de lui communiquer les données personnelles dont il a besoin. Celui-ci en informe l'Autorité de protection des données. 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 huit (8) jours.

Pour des raisons d'enquête judiciaire et 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 200.

Lors de la communication des données à caractère personnel, cette opération comporte 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 la prospection.

Section 2 : Du transfert des données personnelles

Article 201.

Les données personnelles sont stockées et/ou hébergées 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 des données constate que l'État ou l'Organisation Internationale en question assure un niveau de protection adéquat et suffisant 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 202.

Le transfert de données personnelles vers un État tiers ou une organisation internationale n'assurant pas un niveau de protection adéquat, est effectué dans un des cas suivants :

1. La personne concernée a expressément donné son consentement au transfert envisagé après avoir été informée des risques que ce transfert pouvait comporter pour elle, notamment de l'absence de niveau de protection adéquat ;
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 une autre personne physique ou morale ;
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 ou d'autres personnes lorsque la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement.
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.

Les points 1, 2 et 3 de ce paragraphe ne sont pas applicables aux activités des autorités publiques dans l'exercice de leurs prérogatives de puissance publique.

Sans préjudice des dispositions de cet article, le Conseil des Ministres peut, et après avis conforme de l'Autorité de protection des données, autoriser un transfert ou un ensemble de transferts de données à caractère personnel vers un État tiers ou une organisation internationale assurant 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 droit correspondants.

CHAPITRE V : DES DONNEES PERSONNELLES SOUMISES A DES REGIMES PARTICULIERS

Article 203.

Le traitement de données personnelles relatives aux infractions, aux condamnations pénales et aux mesures de sûreté connexes est interdit. Il peut être mis en œuvre par :

1. les autorités publiques et ou judiciaires, 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 réglementaires notamment par des avocats ou d'autres conseils juridiques, pour autant que la défense de leurs clients l'exige ;
3. les autres personnes lorsque le traitement est nécessaire à la réalisation de finalités fixées par ou en vertu d'une disposition légale ou réglementaire ;

4. les personnes physiques ou par des personnelles morales de droit public ou de droit privé pour autant que la gestion de leurs propres contentieux l'exige.

Le 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 204.

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 approuve l'ensemble des conditions relatives à la sécurité et à la confidentialité, au retrait ou à la 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 205.

Dans le cas où les finalités pour lesquelles des données personnelles 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 titre.

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 224, 225, 226 et 227 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 206.

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

1. les catégories de personnes, ayant accès aux données personnelles, 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 de la présente ordonnance-loi, 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 V du présent titre.

Article 207.

Lorsque le traitement de données personnelles est exclusivement autorisé par le consentement écrit que ce soit sur 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 personnelles.

Article 208.

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 personnelles après sa mort.

A cet effet, la personne concernée indique les modalités relatives à la conservation, à l'effacement, 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 ne 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 et, le cas échéant, se faire transmettre les données concernant le de cujus et ce, conformément à la législation en la matière.

CHAPITRE VI : DES DROITS DE LA PERSONNE CONCERNEE, DES OBLIGATIONS ET DU CONTROLE DU RESPONSABLE DE TRAITEMENT, DU SOUS-TRAITANT ET DE LEUR PREPOSE DANS LE TRAITEMENT DE DONNEES PERSONNELLES

Section 1 : Des droits de la personne concernée

Article 209.

La personne physique dont les données à caractère personnel fait 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 sur :

- les finalités du traitement ;
- les catégories de données sur lesquelles il porte et les catégories de destinataires auxquels les données sont communiquées ;
- les destinataires ou catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, lorsque cela est possible ;
- l'existence d'une prise de décision automatisée, y compris un profilage, et, au moins dans 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 ;

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

Article 210.

Dans le cas prévu à l'article précédent, 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 donne préalablement 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 211.

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 ;
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 212.

La 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 213.

La 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, 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 d'exploitation 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.

Pour exercer son droit d'opposition, l'intéressé adresse une demande datée et signée, par voie postale ou électronique, au responsable du traitement ou à son représentant. Le responsable du traitement doit communiquer dans les trente (30) 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, soit sur un papier, support numérique 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 du 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 (60)

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 214.

La 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, par voie électronique ou par porteur, datée et signée au responsable du traitement ou à son représentant.

Dans les trente (30) 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 est adressée à l'autorité ayant en charge la protection des données à caractère personnel par l'auteur de la demande.

Dans le cas où une information a été transmise à un tiers, sa rectification ou son annulation est 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 les 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 justifie, sans frais pour le demandeur, qu'il a procédé aux opérations exigées en vertu de l'alinéa précédent.

Article 215.

La personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans un délai de trente (30) jours, des données à caractère personnel la concernant. Le responsable du traitement a l'obligation de les effacer 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. pour respecter une obligation légale à laquelle le responsable du traitement est soumis ;
3. pour exécuter une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ;
4. les données à caractère personnel ont fait l'objet d'un traitement illicite ;
5. la personne concernée retire le consentement sur lequel est fondé le traitement et il n'existe pas d'autres fondements juridiques au traitement.

Article 216.

Lorsque le responsable du traitement a rendu publiques les données à caractère personnel de la personne concernée, il prend toutes les mesures appropriées, 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 Titre.

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 ci-dessus 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. au respect d'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. à 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 ;
5. à la constatation, à l'exercice ou à la défense de droits en justice.

Article 217.

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 les critères applicables à la limitation du traitement des données à caractère personnel.

Article 218.

En ce qui concerne les traitements relatifs à la sûreté de l'État, 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. L'Autorité de protection des données transmet le rapport de vérification aux services requérants 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 les finalités, la sûreté de l'Etat, 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 met pas en cause les fins qui lui sont assignées, l'Autorité de protection des données prévoit que ces informations sont communiquées au requérant par le gestionnaire du fichier directement saisi dans un délai de trente jours suivant la réception de la demande.

Section 2 : Des obligations de responsables du traitement de données personnelles

Article 219.

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

1. Tenir à jour les 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 186 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 des agents qui s'occupent au quotidien du traitement de données à 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 informatique, 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 soit vérifiée et constatée l'identité des tiers auxquels des données peuvent être transmises par des installations de transmission ;
14. Garantir que soit vérifiée et constatée à posteriori l'identité des personnes ayant eu accès au système informatique 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 220.

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, notamment les informations suivantes :

1. Identité et coordonnées du responsable du traitement ou du délégué à la protection des données et, le cas échéant, du représentant du responsable du traitement ;
2. 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 ;
3. Les catégories de données concernées ;
4. Les destinataires auxquels les données sont susceptibles d'être communiquées ;
5. Le fait de pouvoir demander à ne plus figurer sur le fichier ;
6. 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 ;
7. Le caractère obligatoire ou non de la réponse, le caractère réglementaire ou contractuel ainsi que les conséquences éventuelles d'un défaut de réponse ;
8. L'existence d'un droit d'accès à l'information aux données la concernant et de demande de mise à jour de ses données ;
9. 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 ;
10. Le droit d'introduire une réclamation auprès de l'Autorité ;
11. La durée de conservation des données ;
12. L'existence d'une prise de décision automatisée, y compris un profilage et, en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que !'importance et les conséquences prévues de ce traitement pour la personne concernée ;
13. l'éventualité de tout transfert de données a destination d'Etats tiers.

Article 221.

Le responsable de traitement met en œuvre les moyens nécessaires pour garantir la sécurité des données personnelles, 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 préposés traitant ces données.

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

Lorsque deux responsables du traitement ou plus déterminent conjointement les finalités et les moyens du traitement, ils sont les responsables conjoints du traitement. Les responsables conjoints du traitement définissent de manière transparente leurs obligations respectives afin d'assurer le respect des exigences de la présente ordonnance-loi, notamment en ce qui concerne l'exercice des droits de la personne concernée, et leurs obligations respectives par voie d'accord entre eux. Un point de contact pour les personnes concernées peut être désigné dans cet accord.

L'accord visé à l'alinéa 3 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, la personne concernée peut exercer les droits que lui confère la présente ordonnance-loi à l'égard et contre chacun des responsables du traitement.

Article 222.

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 délégué est chargé notamment de :

1. Assurer, d'une manière indépendante, l'application interne des dispositions de la présente ordonnance-loi ;
2. Tenir un registre des traitements effectués par le responsable du traitement, contenant les informations visées à l'article 168 de la présente ordonnance-loi.

Article 223.

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

Article 224.

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

1. S'assure que le sous-traitant sélectionné remplit toutes les conditions requises par la loi en vigueur sur la sous-traitance ;
2. S'assure que le sous-traitant sélectionné, remplit les garanties suffisantes au regard des mesures de sécurité, éthiques et d'organisation relatives aux traitements ainsi que les mesures techniques et opérationnelles 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. Veille 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. Fixe 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. Convient 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. Consigne par écrit ou sur un support électronique les éléments du contrat visés dans le présent article.

Article 225.

Le responsable du traitement veille et aide à ce que le délégué à la protection des données soit associé, de manière appropriée et en temps utile, à toutes les questions relatives à la protection des données personnelles et exerce les missions qui lui sont dévolues.

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 exécute d'autres missions et tâches. Le responsable du traitement ou le sous-traitant veille à ce que ces missions et tâches n'entraînent pas de conflit d'intérêt.

Article 226.

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 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 227.

Le 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 228.

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

Les obligations de tenir un registre et de désigner un délégué ne s'appliquent pas aux petites et moyennes entreprises ainsi que aux startups, 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.

Section 3 : Des obligations du sous-traitant

Article 229.

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

Le traitement par un sous-traitant est régi par un contrat qui lie le sous-traitant au responsable du traitement, définit l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées, et les obligations et les droits du responsable du traitement.

Ce contrat prévoit, notamment, que le sous-traitant :

- ne traite les données à caractère personnel que sur instruction documentée du responsable du traitement, y compris en ce qui concerne les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale ;
- veille à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité ;
- tient compte de la nature du traitement, aide le responsable du traitement, par des mesures techniques et organisationnelles appropriées, dans toute la mesure du possible, à s'acquitter de son obligation de donner suite aux demandes dont les personnes concernées le saisissent en vue d'exercer leurs droits prévus au présent titre ;
- aide le responsable du traitement à garantir le respect des obligations prévues par le présent titre compte tenu de la nature du traitement et des informations à la disposition du sous-traitant ;
- met à la disposition du responsable du traitement toutes les informations nécessaires pour démontrer le respect des obligations prévues au présent article et pour

permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et contribue à ces audits.

Le sous-traitant ne recrute pas un autre sous-traitant sans l'autorisation écrite préalable, spécifique ou générale, du responsable du traitement. Dans le cas d'une autorisation écrite générale, le sous-traitant informe le responsable du traitement de tout changement prévu concernant l'ajout ou le remplacement d'autres sous-traitants, donnant ainsi au responsable du traitement la possibilité d'émettre des objections à l'encontre de ces changements.

Article 230.

Le 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 peuvent être sous forme matérialisée ou dématérialisée.

Article 231.

Le sous-traitant ou son représentant, le cas échéant, 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 désigner un délégué ne s'appliquent pas aux petites, moyennes entreprises et startups 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 des catégories particulières ou des données à caractère personnel relatives à des condamnations pénales.

Article 232.

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

Section 4 : Des obligations du préposé

Article 233.

La 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.

Section 5 : Du contrôle du traitement des données personnelles

Article 234.

Le contrôle du traitement des données à caractère personnel effectué 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 à caractère personnel.

Cette prérogative ne peut être déléguée à un organe tiers, sauf si l'organe remplit les conditions ci-après :

1. démontre, à la satisfaction de l'autorité de protection des données à caractère personnel, son indépendance et son expertise ;
2. établit des procédures lui permettant d'apprécier si les responsables du traitement et les sous-traitants concernés satisfont aux conditions de contrôle du respect des dispositions et d'examiner périodiquement son fonctionnement ;
3. établit des procédures et des structures pour traiter les réclamations relatives aux violations par un responsable du traitement ou un sous-traitant ;
4. démontre, à la satisfaction de l'autorité ayant en charge de 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 plus réunies ou si les mesures prises par l'organe constituent une violation des dispositions du présent Livre.

Article 235.

Lorsque les données à caractère personnel n'ont pas été collectées auprès de la personne concernée, le responsable du traitement ou son représentant fournit, à la personne concernée, sauf si elle en est déjà informée, les informations ci-après :

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'États 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 ;
- 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 dans 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.

Les informations mentionnées ci-dessus doivent être fournies lors de l'enregistrement des données ou, si la communication de données à un tiers est envisagée, au plus tard au moment de la première communication des données.

Le responsable du traitement fournit les informations visées au premier alinéa :

1. dans un délai raisonnable après avoir obtenu les données à caractère personnel, mais ne dépassant pas trente (30) 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 sur cette autre finalité et toute autre information pertinente visée à l'alinéa 1er.

Article 236.

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

1. L'information de la personne concernée se révèle impossible ou implique des efforts disproportionnés 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 ;
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 légale ou réglementaire.

Article 237.

Le responsable du traitement prend des mesures appropriées pour fournir toute information requise pour procéder à la 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 pout toute information concernant un mineur.

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 238.

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 239.

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

Article 240.

Aucun paiement n'est exigé pour fournir les informations en vue de procéder à toute communication.

Article 241.

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 242.

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 243.

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 place des 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 244.

Le responsable du traitement doit notifier, sans délai, à l'Autorité de protection des données et à la personne concernée toute violation des données à caractère personnel 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 245.

Lorsqu'un 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 ;
2. le traitement à grande échelle des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que du traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique ;
3. le traitement à grande échelle des données relatives à des condamnations pénales et à des infractions ;
4. 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 établit et publie une liste des types d'opérations de traitement pour lesquelles aucune analyse d'impact relative à la protection des données n'est requise.

Article 246.

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 (8) 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.

Article 247.

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 vérifie, dans 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 248.

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 conjoint(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 249.

Sans préjudice de tout autre recours administratif ou juridictionnel, la 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 250.

La personne concernée a le droit de former un recours effectif devant la juridiction administrative compétente lorsque l'autorité en charge de 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 (60), de l'état d'avancement ou de l'issue de la réclamation qu'elle a introduite au titre de l'article précédent.

Article 251.

La personne concernée a, contre le responsable de traitement des données ou son sous-traitant, 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 252.

La 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.

Le 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 s'il a agi en dehors des instructions licites du responsable du traitement ou contrairement à celles-ci.

Le responsable du traitement ou le 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 de traitement ou sous-traitants ou lorsque, à la fois, un responsable de 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.

Lorsque le responsable du traitement ou le 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.

Article 253.

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.

Article 254.

L'interconnexion des fichiers de données personnelles permet 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 inappropriées et doit en outre tenir compte du principe de pertinence des données faisant l'objet de l'interconnexion.

CHAPITRE VII : DES MESURES ADMINISTRATIVES

Article 255.

Constituent notamment 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 stratégiques, 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 256.

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 257.

Lorsque le responsable du traitement ne se conforme pas aux dispositions relatives à la mise en demeure 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. paiement de huit millions à deux cents millions de francs congolais si la violation n'a eu aucun impact grave sur l'État et/ou les personnes concernées;
2. paiement de 5% de son chiffre d'affaires annuel hors taxe de l'exercice écoulé, si la violation a conduit à la mort ou à la tentative de meurtre d'une ou plusieurs personnes;
3. injonction de cesser le traitement des données à caractère personnel, si la violation a mis en danger la sécurité et la sûreté nationale et/ou a conduit à un crime de masse ou à un génocide.

L'État se garde le droit d'intenter une action pénale contre le responsable de traitement et de réclamer des dommages et intérêts contre lui et les personnes concernées.

Article 258.

La 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 (8) jours, à toute modification ou suppression utile dans le fonctionnement des traitements de données à caractère personnel, objet de la sanction.

Article 259.

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 (15) 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 260.

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

Article 261.

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

TITRE IV : DE L'AUTORITE DE PROTECTION DES DONNEES

Article 262.

Il est créée une autorité de protection des données, dénommée Autorité de protection des données en sigle « APD », 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 publiques et à caractère personnel hébergées en République Démocratique du Congo.

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

Un décret du Premier Ministre délibéré en Conseil des Ministres, sur proposition du Ministre ayant le numérique dans ses attributions, fixe l'organisation et le fonctionnement de l'Autorité de protection des données.

Article 263.

L'Autorité de protection des données a pour mission de veiller à ce que le traitement des données publiques et à caractère personnel soit mis en œuvre conformément aux dispositions du Livre III de la présente ordonnance-loi.

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

1. Répondre à toute demande d'avis ou recommandation portant sur un traitement de données publiques et personnelles ;
2. 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 publiques et personnelles ;
3. Informer les personnes concernées et les responsables de traitements de leurs droits et obligations ;
4. Autoriser ou refuser les traitements de fichiers dans un certain nombre de cas, notamment les fichiers sensibles ;
5. Recevoir les formalités préalables à la création de traitements des données personnelles et le cas échéant autoriser ces traitements ;
6. 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 personnelles 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. 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 informer la personne concernée, si elle l'a saisie d'une réclamation, du résultat de ses enquêtes dans un délai raisonnable ;
8. Informer sans délai l'autorité judiciaire pour certains types d'infractions dont elle a connaissance ;
9. 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. Informer l'Assemblée nationale, le Gouvernement ou d'autres institutions politiques, ainsi que le public, de toute question relative à la protection des données publiques et personnelles ;
11. 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. 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. Veiller au respect des autorisations et consultations préalables ;
14. 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. 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. Prononcer des sanctions administratives et pécuniaires, à l'égard des responsables de traitement ;
17. Mettre à jour un répertoire des traitements des données à caractère personnel et le mettre à disposition du public ;
18. Surveiller les faits nouveaux présentant un intérêt, dans la mesure où ils ont une incidence sur la protection des données publiques et personnelles, notamment l'évolution des technologies de l'information et des communications et celle des pratiques commerciales ;
19. Autoriser et surveiller les opérations de monétisation des données ;
20. 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 à son sous-traitant de remédier à cette violation par des mesures déterminées, afin d'améliorer la protection de la personne concernée ;
21. 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 ;
22. Autoriser ou refuser des transferts transfrontaliers de données à caractère personnel vers des États tiers ;
23. 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 ;
24. 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 ;

25. Homologuer les codes de conduite et recueillir et autoriser, le cas échéant, les projets, modifications ou prorogations desdits codes ;
26. Mettre en place des mécanismes de coopération avec les autorités de protection des données publiques et personnelles d'États tiers pour le partage d'informations et l'assistance mutuelle ;
27. Participer aux négociations internationales en matière de protection des données publiques et personnelles ;
28. Assurer le renforcement de capacités des responsables de traitement ou leurs délégués, des sous-traitants et leurs préposés.

Pour l'accomplissement de ses missions, l'Autorité de protection des données peut procéder par voie de recommandations et prendre des décisions individuelles dans les cas prévus par la présente ordonnance-loi.

Article 264.

Les organes de l'Autorité de protection des données sont :

1. L'Assemblée plénière ;
2. Le Bureau ;
3. Les Commissions permanentes.

L'Autorité de protection des données dispose d'un Secrétariat technique chargé des questions administratives, juridiques et financières. Elle a une antenne dans chaque chef-lieu de province, chaque ville et au chef-lieu de territoire.

Article 265.

L'Assemblée plénière comprend l'ensemble des membres de l'Autorité de protection des données. Elle est l'organe de conception, d'orientation, de décision et de contrôle de l'Autorité. Ses décisions sont prises par consensus ou à défaut par vote majoritaire.

Article 266.

L'Assemblée plénière est composée de neuf (9) membres choisis en raison de leurs compétences et/ou techniques ainsi qu'il suit :

1. Une personnalité désignée par le Président de la République ;
2. Trois personnalités désignées par l'Assemblée nationale ;
3. Deux magistrats de carrière désignés par le Conseil Supérieur de la Magistrature ;
4. Un avocat désigné par l'Ordre national des avocats ;
5. Un délégué désigné par la Commission nationale des Droits de l'homme, CNDH en sigle ;
6. Un représentant des organisations patronales issu de l'écosystème numérique, sous réserve des dispositions de l'article 268 de la présente ordonnance-loi.

La désignation des membres tient compte de leur expertise dans le secteur du numérique et de la représentation nationale, ainsi que celle de la femme.

Article 267.

Nul ne peut être désigné membre de l'Assemblée plénière de l'Autorité de protection des données s'il ne remplit pas les conditions ci-après :

1. Être de nationalité congolaise ;
2. Jouir de ses droits civils et politiques ;
3. Être titulaire d'un diplôme de licence au moins ou d'un titre équivalent et justifier d'une expérience professionnelle de 5 ans ou plus dans un domaine pouvant présenter un intérêt pour l'Autorité de protection des données ;
4. Ne pas se trouver dans un des cas d'incompatibilité visés à l'article 268 de la présente ordonnance-loi.

Article 268.

Les membres de l'Assemblée plénière sont nommés par Ordonnance du Président de la République sur proposition du Ministre ayant le numérique dans ses attributions pour une durée de 5 ans renouvelable une fois et sont soumis au contrôle parlementaire.

Les membres de l'Assemblée plénière jouissent d'une immunité totale pour les opinions émises dans l'exercice de leurs fonctions. Ils sont justiciables devant la Cour de Cassation.

La qualité des membres de l'Assemblée plénière est incompatible avec la qualité des membres du Gouvernement, des Députés et Sénateurs, de l'exercice des fonctions de dirigeant d'entreprises, de la détention de participation dans les entreprises du secteur du numérique, bancaire ou des télécommunications.

Article 269.

Le Bureau est l'organe de gestion et de coordination de l'Autorité de protection des données. Il est composé de quatre membres : un Président, un Vice-Président, un Rapporteur et un Rapporteur-Adjoint. Les membres du Bureau de l'Assemblée plénière sont élus par leurs pairs à la majorité simple des voix.

Article 270.

Les Commissions sont des organes techniques chargés de traiter des questions relatives à la mission de l'Autorité de protection des données.

Chaque Commission est dirigée par un membre de la plénière autre que les membres du Bureau de la plénière.

Le nombre des commissions, leur composition, organisation et fonctionnement sont déterminés par décret du Premier Ministre visé à l'article 262 de la présente ordonnance-loi.

LIVRE IV : DE LA SÉCURITÉ ET DE LA PROTECTION PÉNALE DES SYSTÈMES INFORMATIQUES

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

Article 271.

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

Elles fixent également le cadre institutionnel, les règles et modalités d'utilisation de la cryptologie en République Démocratique du Congo.

Article 272.

Le présent Livre s'applique :

1. Aux moyens permettant d'assurer la protection et l'intégrité des systèmes informatiques, des opérateurs d'importance vitale ainsi que des données numériques ;
2. Aux infractions spécifiques liées aux activités et services numériques, ainsi qu'à celles commises sur et au moyen d'un système informatique ;
3. Aux infractions commises dans le cyberespace et dont les effets se produisent sur le territoire national ;
4. À la collecte des preuves électroniques de toute infraction ;
5. Au cadre institutionnel et aux règles procédurales spécifiques à la cybersécurité et à la cybercriminalité en République Démocratique du Congo.

Article 273.

Les dispositions du présent livre ne s'appliquent pas :

1. Aux moyens de chiffrement utilisés par les missions diplomatiques et consulaires conformément aux traités et conventions régulièrement ratifiés ainsi que ceux relatifs à la sécurité intérieure et extérieure.
2. Aux applications et systèmes numériques utilisés par les services spécialisés de défense et de sécurité nationale de la République Démocratique du Congo.

TITRE II : DU CADRE INSTITUTIONNEL

Article 274.

Le cadre institutionnel du secteur de la cybersécurité est l'Agence Nationale de Cybersécurité, « ANCY », en sigle.

L'Agence Nationale de Cybersécurité est l'autorité nationale en charge de la cybersécurité et de la sécurité des systèmes informatiques en République Démocratique du Congo.

CHAPITRE I : DE L'AGENCE NATIONALE DE CYBERSECURITE

Article 275.

L'Agence Nationale de Cybersecurité est un organisme public doté de la personnalité juridique. Elle relève de l'autorité du Président de la République.

Une Ordonnance du Président de la République délibérée en Conseil des Ministres fixe l'organisation et le fonctionnement de l'Agence Nationale de Cybersecurité.

Dans le cadre de ses missions, l'Agence Nationale de Cybersecurité collabore notamment avec les Ministères ayant dans leurs attributions les matières ci-après :

1. l'intérieur et la sécurité ;
2. la défense nationale ;
3. la justice ;
4. le numérique ;
5. les postes et télécommunications ;
6. les droits humains.

Article 276.

L'Agence est l'autorité nationale en charge de la Cybersecurité et de la sécurité des systèmes informatiques en République Démocratique du Congo.

Elle assure la régulation en matière de Cybersecurité, la conformité et l'audit des systèmes informatiques ainsi que des réseaux de communication électronique, l'homologation des prestataires de services et produits de cybersecurité.

L'exploitant d'un système informatique, public ou privé, informe l'Agence Nationale de Cybersecurité de toutes les attaques, intrusions et autres pénétrations susceptibles d'entraver le fonctionnement d'un autre système informatique ou réseau afin de lui permettre de prendre les mesures nécessaires pour y faire face, en ce compris l'isolement du système informatique concerné et cela jusqu'à ce que ces perturbations cessent.

L'exploitant est tenu de se conformer aux mesures édictées par l'Agence Nationale de Cybersecurité pour mettre fin à ces perturbations.

Article 277.

Elle oriente la stratégie nationale de Cybersecurité et propose la politique de sécurité des systèmes informatiques de l'État.

L'Agence Nationale de Cybersecurité apporte son expertise et son assistance technique aux administrations ainsi qu'aux entreprises tant publiques que privées, avec une mission renforcée au profit des infrastructures critiques et essentielles et des opérateurs d'importance vitale (OIV).

Article 278.

L'Agence Nationale de Cybersecurité est chargée notamment des missions suivantes :

- piloter, coordonner et suivre la mise en œuvre de la Stratégie Nationale de Cybersecurité ;
- mettre en place des mesures de prévention, de protection et de défense des données, des infrastructures critiques et essentielles ainsi que celles des réseaux de

communications électroniques face aux risques de cybermenaces en République Démocratique du Congo ;

- piloter la gestion des risques au niveau national, les mesures de cyber-résilience, de gestion des cyber-incidents, de continuité d'activités, de gestion de crises cybers ;
- assurer la conformité des procédures de cybersecurité pour les organismes et institutions publiques ;
- s'assurer du mécanisme d'inclusion nationale des différentes parties prenantes à la mise en œuvre de la stratégie nationale de la Cybersecurité ;
- identifier, en collaboration avec les Ministères et les régulateurs sectoriels, les organismes à importance vitale et les services essentiels, et s'assurer de leur mise à jour ;
- suivre les indicateurs de performances en matière de Cybersecurité et sécurité des systèmes informatiques ;
- établir et maintenir des bases de données des cyber-vulnérabilités ;
- participer au développement de la confiance numérique ;
- assurer l'audit et la veille technologique des systèmes informatiques et des réseaux de communications électroniques en République Démocratique du Congo ;
- certifier et homologuer les produits et services de Cybersecurité et de cryptologie en République Démocratique du Congo ;
- accompagner et collaborer dans la lutte contre la Cybercriminalité avec d'autres organismes et institutions publiques ;
- collaborer et participer à la sensibilisation, à la formation ainsi qu'aux investigations en matière de cybersecurité ;
- assurer la gestion du Fonds souverain ;
- contribuer, en ce qui concerne ses missions, à l'application des accords, traités et conventions relatifs à la Cybersecurité et à la lutte contre la Cybercriminalité ratifiés par la République Démocratique du Congo ;
- veiller à l'exécution des dispositions légales et règlementaires relatives à la sécurité des systèmes informatiques et des réseaux de communication électronique ;
- centraliser les demandes d'assistance à la suite des incidents de sécurité sur les systèmes informatiques et les réseaux de communication électronique.

Article 279.

Il est créé un Fonds souverain de Cybersecurité et des systèmes informatiques, dénommé « Fonds souverain ».

Le Fonds souverain participe au financement de la Stratégie Nationale de Cybersecurité et appuie les activités de l'Agence Nationale de la Cybersecurité.

Un Décret du Premier Ministre délibéré en Conseil des ministres, sur proposition du Ministre ayant le numérique dans ses attributions, définit les modalités de fonctionnement du Fonds souverain ainsi que son financement.

Article 280.

Les systèmes informatiques relevant du secteur public sont soumis à un régime d'audit obligatoire et périodique de la sécurité informatique.

Les critères relatifs à la nature de l'audit, à sa périodicité et aux procédures de l'application des recommandations contenues dans le rapport d'audit, les conditions et procédures d'identification des experts sont fixés par arrêté du Ministre ayant le numérique dans ses attributions. Pour réaliser l'audit visé au présent article, l'Agence Nationale de Cybersecurité et/ou les Experts désignés par celle-ci pour opérer ledit audit, ont le droit de consulter toutes les bases de données, les documents, fichiers et dossiers relatifs à la sécurité informatique afin d'accomplir leurs missions.

Les agents assermentés de l'Agence Nationale de Cybersecurité chargés de l'enquête ont la qualité d'officier de police judiciaire à compétence restreinte. Ils prêtent serment selon les dispositions du droit commun applicables en la matière.

À ce titre, en dehors du rapport administratif adressé à l'Autorité hiérarchique, ils adressent le rapport judiciaire à l'Officier du Ministère public du ressort.

TITRE III : DE LA SÉCURITÉ DES SYSTÈMES INFORMATIQUES

CHAPITRE I : DES OBLIGATIONS GENERALES ET SPECIFIQUES

Section 1 : Des obligations générales

Article 281.

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

Article 282.

Le fournisseur de services en ligne est tenu 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.

Il est également tenu 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 par la présente ordonnance-loi.

L'Officier du Ministère Public ou l'Autorité de protection des données 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 à alinéa 1 du présent article.

Article 283.

Le fournisseur de services en ligne n'est pas responsable du contenu des informations qu'ils transmettent et auxquelles ils donnent accès s'il satisfait aux conditions suivantes :

1. ne pas être à l'origine de la transmission ;
2. ne pas sélectionner le destinataire de la transmission ;
3. ne pas modifier les informations faisant l'objet de la transmission ;
4. 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.

Le fournisseur d'accès à internet et le fournisseur de services en ligne visés à 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 nécessaire à la transmission.

Article 284.

Le fournisseur d'accès à internet et le fournisseur de services en ligne n'engagent pas leur responsabilité civile et/ou pénale 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 285.

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, post-nom, 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 le 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 286.

Le fournisseur d'accès à internet et le fournisseur 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, de l'Agence Nationale de Cybersecurité, les services de sécurité et de maintien de l'ordre public.

Article 287.

Le fournisseur d'accès à internet et le fournisseur de services en ligne concourent à la lutte contre les infractions prévues dans la présente ordonnance-loi.

Ils mettent en place, à ce titre, 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 suspendre tout contenu susceptible de porter atteinte à la moralité.

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 288.

La personne dont l'activité est d'éditer un service de communication au public en ligne, est tenue de mettre à la disposition de ses abonnés, dans un standard ouvert, les noms du directeur de publication et du responsable de la rédaction, la dénomination sociale, l'adresse électronique ainsi que le numéro de téléphone du fournisseur de services en ligne.

Article 289.

Le fournisseur d'accès a internet et le fournisseur de services en ligne sont tenus a 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 a l'autorité judiciaire, ni aux services d'enquête de la police judiciaire, ni à l'Agence Nationale de Cybersécurité, 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 290.

Le fournisseur de cache n'est pas responsable des données et informations qu'il traite dans le cadre de ses activités.

Toutefois, il devient responsable dans les conditions suivantes s'il :

1. modifie l'information ;
2. ne se conforme pas aux conditions d'accès à l'information ;
3. ne se conforme pas aux règles concernant la mise à jour de l'information, indiquées d'une manière largement reconnue et utilisée dans le secteur ;
4. entrave 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 ;
5. n'agit pas promptement pour retirer l'information stockée ou pour rendre l'accès à celle-ci impossible dès qu'il a effectivement connaissance du fait que l'information à l'origine de la transmission a été retirée du réseau ou du fait que l'accès à l'information a été rendu impossible, ou du fait qu'une autorité administrative ou judiciaire a ordonné de retirer l'information ou de rendre l'accès à cette dernière impossible.

Article 291.

Le fournisseur de liens hypertextes est responsable des informations auxquelles il donne accès, dès lors que :

1. il ne supprime ou n'empêche pas rapidement l'accès aux informations après avoir reçu une injonction de l'autorité judiciaire de retirer le lien hypertexte ;
2. il n'a pas 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 ;

3. il n'a pas informé 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 292.

Le fournisseur de moteurs de recherche qui, de manière automatique ou sur la base des entrées effectuées par autrui, présente un index des contenus en ligne ou met à disposition des moyens électroniques pour rechercher les informations fournies par des tiers, est responsable des résultats de recherche, à condition qu'il :

1. soit à l'origine de la transmission ;
2. sélectionne le destinataire de la transmission ;
3. sélectionne ou modifie les informations contenues dans la transmission.

Article 293.

L'hébergeur est responsable des informations stockées à la demande d'un utilisateur du service qu'il fournit, à condition que :

1. lorsqu'il n'a pas pris connaissance d'informations illégales spécifiques, stockées ou des activités illégales qu'exerceraient les destinataires du service, il en informe immédiatement l'autorité judiciaire.
2. Il ne retire pas, ne rend pas l'accès impossible ou ne désactive pas 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 294.

Le vendeur de produits et/ou fournisseur de services des technologies de l'information et de la communication est tenu de solliciter, auprès du Ministre ayant le numérique dans ses attributions, un certificat de conformité après analyse de la vulnérabilité et évaluation de la garantie de sécurité par des experts en sécurité informatique agréés par ledit Ministre.

Il est, en outre, tenu d'informer les consommateurs de toutes les vulnérabilités décelées dans les produits et services des technologies de l'information et de la communication ainsi que des solutions déployées pour y remédier.

Article 295.

Le fournisseur des services numériques est tenu de mettre en œuvre des systèmes qualifiés de détection des événements susceptibles d'affecter la sécurité de leurs systèmes informatiques.

Les qualifications des systèmes de détection et des prestataires de services exploitant ces systèmes sont délivrées par le Ministère ayant le numérique dans ses attributions, l'Agence Nationale de Cybersecurité entendue.

Article 296.

Le fournisseur des services numériques soumet son système informatique 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 Cybersecurité. Le coût des contrôles est à la charge du fournisseur des services numériques.

Article 297.

Pour les besoins de la sécurité des systèmes informatiques et des fournisseurs de services numériques, l'Agence Nationale de Cybersecurité peut obtenir des fournisseurs, l'identité, l'adresse postale et l'adresse électronique d'utilisateurs ou de détenteurs de systèmes informatiques vulnérables, menacés ou attaqués, afin de les alerter sur la vulnérabilité ou la compromission de leur système.

CHAPITRE II : DE LA CRYPTOLOGIE

Section 1 : Des dispositions générales

Article 298.

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.

Toutefois, 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.

Section 2 : Du régime juridique

Article 299.

Nul ne peut opérer une activité de cryptologie sans se soumettre à l'un des régimes juridiques prévus dans le présent Livre.

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 de la présente ordonnance-loi 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 des charges relève de l'Agence Nationale de Cybersecurité.

L'Agence Nationale de Cybersecurité crée en son sein une Commission de cryptologie.

Article 300.

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 de cryptologie de l'Agence Nationale de Cybersecurité, sous réserve des éventuelles dispenses de déclaration en vertu d'une disposition légale ou réglementaire.

Article 301.

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 de cryptologie une description des caractéristiques techniques des moyens de cryptologie utilisés.

Article 302.

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 de cryptologie de l'Agence Nationale de Cybersecurité entendue.

Section 3 : Des prestataires de services de cryptologie

Article 303.

Le prestataire de services de cryptologie est tenu d'obtenir une autorisation préalable auprès de la Commission de cryptologie de l'Agence Nationale de Cybersecurité.

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 304.

La Commission de cryptologie de l'Agence Nationale de Cybersecurité, sur instruction du Ministre ayant le numérique dans ses attributions, prévoit 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'État, cette fourniture peut être dispensée de toute formalité préalable.

Article 305.

Le prestataire de services de cryptologie est 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 au service de cryptologie fourni. Toute clause contractuelle contraire est réputée non écrite.

Le prestataire de services de cryptologie dégage ou limite sa responsabilité s'il parvient à démontrer l'absence de négligence ou de faute intentionnelle.

Le prestataire de services de cryptologie est exonéré de toute responsabilité à l'égard des personnes qui font un usage non autorisé de leurs services, pour autant que les conditions d'utilisation contenues dans une déclaration écrite soient accessibles aux utilisateurs et présentent clairement les usages autorisés et non autorisés.

Le prestataire de services de cryptologie doit obligatoirement contracter une police d'assurance couvrant les risques liés à l'exercice de leurs activités.

Section 4 : Des sanctions administratives

Article 306.

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, l'Agence Nationale de Cybersecurité 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.

Article 307.

L'interdiction de mise en circulation prévue à l'article précédent 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 est remis en circulation dès que les obligations antérieurement non respectées auront été satisfaites.

TITRE IV : DE LA PROTECTION PÉNALE DES SYSTÈMES INFORMATIQUES

CHAPITRE I : DES PRINCIPES GENERAUX

Section 1 : De la responsabilité pénale

Article 308.

L'État, 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 punies par la présente ordonnance-loi dans l'exercice de leurs fonctions.

Article 309.

La personne morale de droit privé est responsable des infractions prévues par les dispositions de la présente ordonnance-loi 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'ils commettent des infractions dans les mêmes circonstances et dans l'exercice de leurs fonctions.

Section 2 : Des peines

Article 310.

Sans préjudice des dispositions du Code pénal congolais, les peines applicables en matière d'infractions relatives à la cybercriminalité sont :

1. La servitude pénale ;
2. L'amende ;
3. La confiscation spéciale.

Article 311.

Les peines encourues par les personnes morales, pour les infractions visées à la présente ordonnance-loi, sont les suivantes :

1. Une amende dont le montant maximum est égal au quintuple de celui prévu pour les personnes physiques par la loi qui réprime l'infraction ;
2. La dissolution lorsqu'il s'agit d'une infraction qui porte atteinte à la sécurité et à la sûreté de l'État ;
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 pour une durée de deux (2) à cinq (5) 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 tireur ou ceux qui sont certifiés, ou d'utiliser des cartes de paiement ;
8. La confiscation de l'outil ayant servi à commettre l'infraction et du produit de l'infraction.

Article 312.

Sans préjudice des dispositions du Code pénal congolais, en cas de condamnation pour 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 313.

Sans préjudice des dispositions du Code pénal congolais, en cas de condamnation pour l'une des infractions prévues à la présente ordonnance-loi, 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 de cinq (5) à dix (10) ans.

La juridiction compétente peut faire injonction à toute personne responsable 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.

Article 314.

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 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'État 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 paraétatiques quel qu'en soit l'échelon ;
- Droit d'être expert ou témoin dans les actes d'état civil ;
- Droit de déposer en justice, autrement que pour y donner de simples renseignements.

La violation des interdictions prévues dans la présente ordonnance-loi et prononcées par les cours et 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 315.

Est puni de la même peine que !'infraction consommée, et ce conformément au Code pénal Livre I, toute participation criminelle et toute tentative de violation de la présente ordonnance-loi.

Section 4 : De la récidive et des circonstances aggravantes

Article 316.

Lorsqu'une des infractions prévues par la présente ordonnance-loi 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, le maximum de la servitude pénale ne pouvant dépasser vingt ans.

Article 317.

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 la présente ordonnance-loi, la peine initialement prévue est doublée, le maximum de la servitude pénale ne pouvant dépasser vingt ans.

Lorsque l'une des infractions prévues en vertu de la présente ordonnance-loi porte atteinte à la sûreté de l'État, aux données informatiques et/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 à vingt milliards de Francs congolais.

CHAPITRE II : DES REGLES DE PROCEDURE ET DE COMPETENCE DES JURIDICTIONS

Section 1 : De la constatation des infractions a la législation du numérique

Article 318.

Les infractions à la législation du numérique sont constatées par les officiers de police judiciaire à compétence restreinte ou à compétence générale selon le cas.

Lorsque les officiers de police judiciaire sont saisis ou constatent les faits infractionnels aux dispositions de la présente ordonnance-loi, ils en informent l'officier du Ministère public compétent conformément aux dispositions du Code de procédure pénale.

Article 319.

Les infractions à la législation du numérique sont 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 320.

Lorsque des données stockées dans un système informatique ou sur un support permettant de conserver des données sur le territoire national 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 à un autre système informatique ou 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 321.

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 sur décision du juge.

Section 3 : De l'interception des données

Article 322.

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 de la présente ordonnance-loi, y compris des données relatives au contenu, émises par voie de communications électroniques.

L'interception ne peut porter sur une ligne dépendant d'un avocat, du Cabinet d'un avocat ou de son domicile, sauf s'il existe des raisons plausibles de le soupçonner d'avoir commis ou tenté de commettre, en tant qu'auteur ou complice, l'infraction qui fait l'objet de la procédure ou une infraction connexe, à la condition que la mesure soit proportionnée au regard de la nature et de la gravité des faits. L'interception est autorisée par décision du Procureur Général près la Cour d'Appel, saisi par réquisition du Magistrat poursuivant, le bâtonnier national informé ou le bâtonnier selon le cas.

Article 323.

L'Agence Nationale de Cybersecurité autorise :

1. les interceptions de correspondances émises par la voie des communications électroniques, conformément aux dispositions de la présente ordonnance-loi ;

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 273 de la présente ordonnance-loi.

Les modalités de mise en œuvre des dispositions du présent article seront précisées par voie réglementaire.

Article 324.

Les opérations d'interception visées par la présente ordonnance-loi sont autorisées par l'Agence Nationale de Cybersecurité lorsqu'elles sont nécessaires :

1. au maintien de la souveraineté 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 325.

Les infractions à la législation du numérique sont poursuivies conformément au Code de procédure pénale et prouvées par toute voie de droit.

Article 326.

L'action publique contre les infractions à la législation du numérique est exercée conformément au Code de procédure pénale et aux dispositions de la présente ordonnance-loi.

Section 5 : De l'extinction de l'action publique

Article 327.

L'action publique en répression des infractions à la législation du numérique se prescrit conformément au Code de procédure pénale congolais.

Les 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.

Section 6 : Des juridictions compétentes

Article 328.

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 la présente ordonnance-loi qui portent atteinte à la législation économique et commerciale, quel que soit le taux de la servitude pénale ou le montant de l'amende.

Article 329.

Sans préjudice du code de procédure pénale, 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, ou 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

Article 330.

Constitue une infraction à la législation du numérique, toute violation de celle-ci passible d'une peine prévue par la présente ordonnance-loi.

La présente ordonnance-loi définit les incriminations et les peines des infractions spécifiques liées au numérique.

Section 1 : Des infractions de droit commun commises au moyen d'un ou sur un réseau de communication électronique ou un système informatique

Article 331.

Les infractions de droit commun commises au moyen d'un réseau de communication électronique ou d'un système informatique sont réprimées conformément au Code pénal congolais et aux dispositions pénales particulières en vigueur.

Section 2 : Des atteintes aux systèmes informatiques

Paragraphe 1 : De l'accès et du maintien illégal

Article 332.

Quiconque accède ou se maintient frauduleusement 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 trois à cinq ans et d'une amende de cinquante millions à cent millions de francs congolais, ou de l'une de ces peines seulement.

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 cinquante millions à cent millions de francs congolais, ou de l'une de ces peines seulement.

Article 333.

Lorsqu'il résulte des faits visés à l'article précédent 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 sont portées de cinq à dix ans de servitude pénale et d'une amende de cent millions à trois cents millions de francs congolais ou de l'une de ces peines seulement.

Lorsque les faits visés à l'article précédent sont commis en violation de mesures de sécurité, l'auteur de ces faits est puni d'une peine de servitude pénale de dix à vingt ans et d'une amende de trois cents millions de francs congolais à cinq cent cinquante millions de francs congolais ou de l'une de ces peines seulement.

Paragraphe 2 : Des atteintes aux données d'un système informatique

Article 334.

Est puni d'une servitude pénale de cinq à dix ans et d'une amende de cinquante à cent 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 335.

Est puni d'une servitude pénale de six mois à trois ans et d'une amende de cinq millions à cent millions de francs congolais, celui qui transfère, sans autorisation de la personne concernée, des données à caractère personnel de cette dernière d'un système informatique ou d'un moyen de stockage de données vers un autre.

La peine prévue à l'alinéa précédent pourra être portée de trois à dix ans de servitude pénale, si 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, ne constitue pas une infraction au sens du présent article :

1. L'interception réalisée conformément à un mandat de justice ;
2. La communication envoyée par ou destinée à une personne qui a consenti à l'interception ;
3. L'interception réalisée par une personne morale légalement autorisée pour les besoins de la sécurité publique ou de la défense nationale ;
4. L'interception réalisée par une personne morale ou physique légalement autorisée en vertu des dispositions légales et réglementaires en vigueur en République Démocratique du Congo.

Article 336.

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 cinquante millions à cent 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 cinquante millions à cent millions de Francs congolais, ou l'une de ces peines seulement.

Paragraphe 3 : Des atteintes à l'intégrité du système informatique

Article 337.

Est puni d'une peine de servitude pénale de cinq à dix ans et d'une amende de deux cents millions à deux cent cinquante 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 dix à quinze ans et d'une amende de deux cents millions à deux cent cinquante 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 empêché, 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 quinze à vingt ans et à une amende de deux cents millions à deux cent cinquante 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 de la présente ordonnance-loi, la personne responsable est condamnée à la peine de servitude pénale de quinze à vingt ans et à une amende de trois cents 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 abus de dispositifs

Article 338.

Quiconque aura, intentionnellement et sans droit, produit, vendu, importé, exporté, diffusé ou mis à disposition sous une autre forme, un quelconque dispositif ou équipement électronique, y compris des données ou des programmes informatiques, principalement conçu ou adapté pour permettre la commission d'une ou plusieurs infractions prévues dans la présente ordonnance-loi, sera puni d'une peine de servitude pénale de deux à cinq ans et d'une amende de deux cents cinquante millions à cinq cents millions de francs congolais ou de l'une de ces peines seulement.

Quiconque, intentionnellement et sans droit, aura possédé au sens de la présente ordonnance-loi, un quelconque dispositif, y compris des données, principalement conçu ou adapté pour permettre la commission d'une ou plusieurs infractions prévues dans la présente ordonnance-loi est puni d'une peine de servitude pénale de six mois 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.

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, 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 la présente ordonnance-loi.

Paragraphe 5 : De la falsification des données ou faux en informatique

Article 339.

Quiconque commet un faux en introduisant, intentionnellement et sans droit, dans un système informatique ou un réseau de communication électronique, en modifiant, en altérant ou en effaçant des données qui sont stockées, traitées ou transmises par un système informatique ou un réseau de communication électronique, ou en modifiant par tout autre moyen technologique, l'utilisation possible des données dans un système informatique ou un réseau de communication électronique, et par là modifie la portée juridique de telles données, est puni d'une servitude pénale de trois à cinq ans

et d'une amende de vingt millions à cinquante millions de francs congolais, ou de l'une de ces peines seulement.

Quiconque fait usage des données visées à l'article précédent, tout en sachant que celles-ci sont fausses, est puni d'une servitude pénale de cinq à dix ans et d'une amende de vingt millions à cinquante millions de francs congolais, ou de l'une de ces peines seulement.

Paragraphe 6 : De la fraude informatiques

Article 340.

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 cinquante à cent 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 l'Agence Nationale de Cybersécurité

Article 341.

Est puni d'une amende de cinq à dix millions de francs congolais, quiconque n'aura pas satisfait à l'obligation de communication à l'Agence Nationale de Cybersecurité d'une description des caractéristiques techniques du moyen de cryptologie dans les conditions prévues par les dispositions du Titre II de la présente ordonnance-loi et de ses textes d'application.

Article 342.

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 l'Agence Nationale de Cybersecurité.

Est puni de cinq à dix ans de servitude pénale et d'une amende de cinquante à cent millions de francs congolais, quiconque aura fourni des prestations de cryptologie sans avoir obtenu préalablement le certificat d'agrément de l'Agence Nationale de Cybersecurité.

Article 343.

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 l'Agence Nationale de Cybersecurité.

Article 344.

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.

Article 345.

Est puni de cinq à dix ans de servitude pénale et d'une amende de cinquante à cent millions de Francs congolais, ou de l'une de ces peines seulement, quiconque par un moyen de cryptologie, aura fait obstacle au déroulement des enquêtes au sens du Code de procédure pénale et de la présente ordonnance-loi ou refusé de fournir des informations ou documents y afférents.

Article 346.

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, la servitude pénale ne pouvant dépasser vingt ans.

Article 347.

Est puni de trois ans de servitude pénale et d'une amende de cinq millions à quarante 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 liées à l'utilisation des données à caractère personnel

Paragraphe 1 : De l'envoi de messages non sollicités

Article 348.

Tout message électronique non sollicité envoyé sur la 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 349.

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 de l'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 traitement non autorisé

Article 350.

Quiconque aura procédé à un transfert de données à caractère personnel soit sans avoir préalablement informé individuellement la personne concernée 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 de l'une de ces peines seulement.

Paragraphe 4 : De l'usurpation d'identité

Article 351.

Est puni d'une servitude pénale d'un an à cinq ans et d'une amende de vingt millions à cent millions de Francs congolais, quiconque usurpe, par hameçonnage, phishing ou tout autre moyen, intentionnellement et sans droit par le biais d'un système informatique, l'identité d'autrui, une ou plusieurs données permettant de s'attribuer faussement et de manière illicite l'identité d'autrui dans le but 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 de deux à cinq ans et d'une amende de cinq à cent millions de Francs congolais ou d'une de ces peines seulement.

Sera puni d'une peine de servitude pénale de cinq à dix ans et d'une amende de cent millions à deux cents millions de francs congolais, ou l'une de ces peines seulement, quiconque se fait passer pour un tiers institutionnel, de confiance ou autre, par le truchement d'un système informatique, dans le but d'inciter ou contraindre la victime à lui communiquer des données personnelles.

Article 352.

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 cinquante millions à cent millions de Francs congolais.

Section 5 : De la fraude aux cartes bancaires et des infractions relatives à la publicité sur internet

Paragraphe 1 : De la fraude aux cartes bancaires

Article 353.

Sans préjudice des autres dispositions prévues à l'article 123 de la loi n° 18/019 du 09 juillet 2018 relative aux systèmes de paiement et règlements-titres, est puni d'une peine de servitude pénale de deux à cinq ans et d'une amende de cinquante à cinq cents 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 354.

Est puni d'une peine de servitude pénale de cinq à dix ans et d'une amende de cinquante millions à cinq cents millions de Francs congolais ou 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 ayant servi ou étant destinés à servir ou étant 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 a la publicité sur Internet

Article 355.

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 du contenu tribaliste, raciste et xénophobe par le biais d'un système électronique

Article 356.

Quiconque aura, intentionnellement créé, téléchargé, diffusé ou mis à la disposition du public par le biais d'un système informatique des écrits, contenus, messages, photos, sons, vidéos, dessins ou toute autre représentation d'idées ou de théories, de nature raciste, tribaliste ou xénophobe ou sous quelque forme que ce soit, au sens de la présente ordonnance-loi 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 : De la pornographie infantile

Article 357.

Le fait de produire, de distribuer, de diffuser, d'importer, d'exporter, d'offrir, de rendre disponible, de vendre, de se procurer ou de procurer à autrui, de posséder tout matériel pornographique mettant en scène un enfant par le biais d'un système informatique ou d'un réseau de communication électronique, est puni de cinq à quinze ans de servitude pénale principale et d'une amende de deux mille à un million de Francs congolais.

Paragraphe 3 : Du harcèlement par le biais d'une communication électronique

Article 358.

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 359.

Quiconque aura harcelé, par le biais d'un système informatique ou d'un réseau de 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 360.

Quiconque initie ou relaie une fausse information contre une personne par le biais des réseaux sociaux, des systèmes informatiques, des réseaux de communication électronique de 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 4 : De la négation, minimisation grossière, approbation ou justification des crimes internationaux ou des violences sexuelles

Article 361.

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 ou d'un réseau de communication électronique des données qui nient, minimisent, approuvent ou justifient des actes constitutifs de crime de génocide, crimes de guerre, de crimes contre l'humanité, des crimes d'agression et/ou des violences sexuelles tels que définis par 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 5 : De l'incitation ou provocation à la commission d'actes terroristes et apologie des actes terroristes

Article 362.

Quiconque aura, au moyen d'un système informatique ou d'un réseau de communication électronique, incité ou provoqué directement des actes de terrorisme, sera puni conformément aux dispositions des articles 157 à 160 du Code pénal militaire congolais.

Paragraphe 6 : Du courrier indésirable ou pourriel ou ou spam

Article 363.

Sera puni d'une servitude pénale de deux à cinq ans et d'une amende de dix à cinquante millions de 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 erronés, indésirables ou contraires à la loi, de courrier électronique multiples à partir ou par l'intermédiaire d'un système informatique ;
2. utilise un système informatique ou un réseau de communication électronique 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 à charge du fournisseur d'accès à internet

Article 364.

Le 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 millions à vingt millions de Francs congolais.

En cas de récidive, l'amende est de dix millions à vingt millions de francs congolais.

Article 365.

La 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 366.

La 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 aux obligations inhérentes à son statut juridique telles que disposées au Livre Ier de la présente ordonnance-loi, 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.

Les mêmes peines prévues à l'alinéa précédent s'appliquent à toute personne physique ou tout dirigeant d'une personne morale, de droit ou de fait, exerçant l'activité d'éditeur de services de communication en ligne qui ne satisfait pas à l'obligation de vigilance prévue au Livre III de la présente ordonnance-loi.

Article 367.

La 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 aux obligations inhérentes à son statut juridique telles que disposées au Livre Ier de la présente ordonnance-loi, est punie d'une amende de cent millions à cinq cents millions de francs congolais.

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 368.

Quiconque aura commis des actes constitutifs d'une infraction de presse, par le biais d'un système informatique ou d'un réseau de communication électronique, sera puni conformément aux dispositions légales applicables à la presse et à la communication.

Article 369.

Sans préjudice des dispositions légales applicables à la presse et à la presse et à la communication, quiconque ayant fait l'objet d'une publication au moyen d'un ou sur un réseau de communication électronique ou un système informatique, dispose d'un droit de réponse, sans préjudice de demandes 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.

À défaut de respecter le prescrit de l'alinéa précédent, le responsable de la publication sera puni d'une amende de deux millions à cinq cents millions de Francs congolais.

Paragraphe 2 : De la divulgation des détails d'une enquête

Article 370.

Est puni d'une servitude pénale d'un mois à deux ans, ou d'une amende de deux millions à cinq millions de Francs congolais ou de l'une de ces peines seulement quiconque, 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 par le biais d'un système informatique ou d'un réseau de communication électronique, 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 et de l'enquête.

Section 9 : Du cyberespionnage

Article 371.

Sera puni d'une servitude pénale de cinq à quinze ans et d'une amende de cinq milliards 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 ou une entreprise étrangère, à un intermédiaire étranger, ou à un agent étranger qualifié d'espion par le biais d'un système informatique :

1. vole, ou, sans autorisation, s'approprie, prend, emporte, ou cache, ou frauduleusement, ou de façon factice, ou par supercherie, obtient soit une information de nature à porter atteinte à la sécurité et sûreté de l'État tel que prévu par les dispositions pénales, soit un secret commercial ou industriel ;

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 à la commission des infractions et de la diffusion des éléments pour fabriquer des engins de destruction

Paragraphe 1 : De l'enregistrement des images relatives à la commission des infractions

Article 372.

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 soit lorsqu'il est réalisé afin de servir de preuve en justice.

Paragraphe 2 : De la diffusion des éléments pour fabriquer des engins de destruction

Article 373.

Quiconque aura diffusé, au moyen d'un réseau de communication électronique ou d'un système informatique, 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 d'un système informatique

Article 374.

Est puni d'une amende de dix à cinquante millions de Francs congolais, le fait pour les responsables des systèmes informatiques, d'omettre de maintenir en bon état les dispositifs de protection d'un système informatique.

Section 11 : De l'atteinte aux droits d'auteur et a la propriété intellectuelle et industrielle ainsi qu'aux droits voisins

Article 375.

Quiconque commet délibérément, à une échelle commerciale et au moyen d'un système informatique, une atteinte aux droits d'auteur, à la propriété intellectuelle et industrielle ainsi qu'aux droits voisins définis par la législation en vigueur en République Démocratique du Congo, est puni de six mois à cinq ans de servitude pénale et d'une amende de cinquante à cent millions de Francs congolais, ou de l'une de ces peines.

Quiconque porte atteinte au droit patrimonial ou au droit de l'auteur d'une création informatique, à savoir un programme informatique, est puni de six mois à cinq ans de servitude pénale et d'une amende de cinquante à cent millions de Francs congolais ou de l'une de ces peines.

Paragraphe 1 : De la contrefaçon de marque, nom commercial, appellation d'origine, indication géographique, logiciel et matériel de conception préparatoire

Article 376.

La contrefaçon et/ou le piratage 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 377.

Est puni d'une servitude pénale de trois à cinq ans et d'une amende de cinquante à cent millions de Francs congolais ou de l'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 378.

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 système informatique. Ceux qui, en toute 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 logiciels ou des matériels informatiques protégés par un brevet d'invention sont punis des mêmes peines prévues à l'article 14 du Code pénal.

Sans préjudice des peines prévues à l'article 14 du Code pénal, sont punis de cinq à dix ans de servitude pénale et d'une amende de deux cents à deux cents cinquante millions de Francs congolais.

Paragraphe 4 : De l'atteinte aux schémas de configuration d'un système numérique protégé

Article 379.

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 communication électronique.

Paragraphe 5 : De l'atteinte a une mesure technique efficace

Article 380.

Est puni d'une amende de vingt-cinq à cinquante millions de Francs congolais, le fait de porter atteinte, à des fins autres que la recherche scientifique, 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 par 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 381.

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 scientifique, 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, en commandant, concevant, organisant, reproduisant, distribuant ou diffusant une publicité en faveur de l'un des précédés visés aux points 1 à 3 au moyen d'un système informatique.

Article 382.

Est puni d'une servitude pénale de deux à six mois et d'une amende de deux millions à cinq millions de 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 scientifique ou de sécurité informatique.

LIVRE V : DES DISPOSITIONS DIVERSES, TRANSITOIRES, ABROGATOIRES ET FINALES

CHAPITRE I : DU REGIME FISCAL, PARAFISCAL, DOUANIER ET DE CHANGER

Article 383.

Les personnes morales et physiques exerçant des activités et services numériques évoluant dans le secteur du numérique à partir ou à destination de la République Démocratique du Congo, sont soumises au régime du droit communs en matière fiscale, parafiscale, douanière et de change en vigueur.

Article 384.

Les startups du numérique, ayant le statut d'entreprenant, sont éligibles aux avantages fiscaux, parafiscaux, douanier et de change prévu par la législation relative à l'entrepreneuriat et aux startups.

En outre, et sans préjudice des dispositions de l'Ordonnance-loi n° 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, entreprenants 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 que d'autres impôts, droits, taxes et redevances indirects pour une période de cinq ans. Exception faite des impôts professionnels sur les rémunérations et mobiliers.

Un arrêté interministériel 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'alinéa 1er du présent article.

Article 385.

L'admission à un des régimes juridiques prévus dans la présente ordonnance-loi 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'État.

Il est ajouté une annexe relative aux droits, taxes et redevances dus au secteur du numérique en complément à l'Ordonnance-loi n° 18/003 du 13 mars 2018 fixant la nomenclature des droits, taxes et redevances du pouvoir central, ainsi libellée :

N°	LIBELLÉ DES DROITS, TAXES ET REDEVANCES	FAIT GÉNÉRATEUR
XXXII. NUMÉRIQUE		
01	Taxe sur l'autorisation de fourniture des services numériques	Demande d'autorisation
02	Taxe sur la déclaration en vue d'un certificat d'agrément pour l'exploitation et la fourniture des services numériques	Déclaration d'exploitation des services numérique
03	Taxe sur l'homologation pour la fourniture des services numériques aux entités publiques	Demande d'homologation

N°	LIBELLÉ DES DROITS, TAXES ET REDEVANCES	FAIT GÉNÉRATEUR
04	Redevance sur le chiffre d'affaires des entreprises de Cybersécurité et de sécurité des systèmes informatiques	Exploitation

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 LA COMMANDE PUBLIQUE

Article 386.

La passation d'un marché public est, outre les dispositions de la présente ordonnance-loi, régie conformément à la loi n° 10/010 du 27 avril 2010 relative aux marchés publics.

Article 387.

L'établissement d'un partenariat public-privé dans le secteur du numérique est, outre les dispositions de la présente ordonnance-loi, régi conformément à la loi n°18/016 du 09 juillet 2018 relative au partenariat public-privé.

CHAPITRE III : DES DISPOSITIONS TRANSITOIRES, ABROGATOIRES ET FINALES

Article 388.

Les fournisseurs de services numériques opérant sur la base de titres obtenus antérieurement à la présente ordonnance-loi sont tenus de se conformer aux nouvelles dispositions de la présente ordonnance-loi dans un délai de six mois à dater de son entrée en vigueur.

Article 389.

Sont abrogées toutes les dispositions antérieures contraires à la présente ordonnance-loi.

Article 390.

La présente ordonnance-loi entre en vigueur à la date de sa promulgation.

Fait à Kinshasa, le 13 mars 2023

Félix-Antoine TSHISEKEDI TSHILOMBO
Président de la République

PLAN DÉTAILLÉ DU CODE

LIVRE PRÉLIMINAIRE : DE L'OBJET, DU CHAMP D'APPLICATION ET DES DÉFINITIONS....3
CHAPITRE I : DE L'OBJET ET DU CHAMP D'APPLICATION....3
CHAPITRE II : DES DEFINITIONS....3
LIVRE PREMIER : DES ACTIVITÉS ET DES SERVICES NUMÉRIQUES....10
TITRE I : DE L'OBJET ET DU CHAMP D'APPLICATION....10
TITRE II : DU CADRE INSTITUTIONNEL....10
CHAPITRE I : DU MINISTERE....10
CHAPITRE II : DE L'AUTORITE DE REGULATION DU NUMERIQUE....11
CHAPITRE III : DE L'AUTORITE NATIONALE DE CERTIFICATION ÉLECTRONIQUE11
CHAPITRE IV : DU CONSEIL NATIONAL DU NUMERIQUE....12
TITRE III : DU RÉGIME JURIDIQUE APPLICABLE AUX ACTIVITÉS ET SERVICES NUMÉRIQUES....13
CHAPITRE I : DES DISPOSITIONS GENERALES....13
CHAPITRE II : DE L'AUTORISATION....13
CHAPITRE III : DE LA DECLARATION....13
CHAPITRE IV : DE L'HOMOLOGATION....14
TITRE IV : DES DROITS, PRINCIPES GÉNÉRAUX ET OBLIGATIONS APPLICABLES AUX FOURNISSEURS DES ACTIVITÉS ET SERVICES NUMÉRIQUES....14
CHAPITRE I : DES DROITS ET PRINCIPES GÉNÉRAUX APPLICABLES AUX FOURNISSEURS DES ACTIVITÉS ET SERVICES NUMÉRIQUES....14
CHAPITRE II : DES OBLIGATIONS DES FOURNISSEURS DES ACTIVITÉS ET SERVICES NUMÉRIQUES....16
TITRE V : DE L'ADMINISTRATION DÉMATÉRIALISÉE....18
CHAPITRE I : DES ECHANGES D'INFORMATION AU SEIN DE L'ADMINISTRATION PUBLIQUE....18
CHAPITRE II : DU GUICHET NUMERIQUE....18
TITRE VI : DE L'ARCHIVAGE ÉLECTRONIQUE....19
CHAPITRE I : DISPOSITIONS GENERALES....19
CHAPITRE II : DES ARCHIVES NUMERIQUES PUBLIQUES....19
TITRE VII : DES DROITS DE LA PROPRIETE INTELLECTUELLE ET INDUSTRIELLE....20
CHAPITRE I : DISPOSITIONS GENERALES....20
TITRE VIII : DU COMMERCE ÉLECTRONIQUE....20
CHAPITRE I : DISPOSITIONS GENERALES....20
Section 1 : De l'objet et du champ d'application....20
Section 2 : Des principes régissant le commerce électronique....20
CHAPITRE II : DE LA CONCLUSION DU CONTRAT SOUS FORME ELECTRONIQUE...21
Section 1 : Principe et contenu de l'offre....21
Section 2 : Conditions de validité d'un contrat conclu par voie électronique....22
Section 3 : Responsabilité contractuelle des parties....23
CHAPITRE III : DE L'EXECUTION DU CONTRAT ELECTRONIQUE....23
Section 1 : Du paiement du prix, de la livraison du produit et de la prestation des services....23
Section 2 : De l'obligation de conserver les registres des transactions....24
CHAPITRE IV : DU DROIT DE RETRACTATION....24
Section 1 : Délai de rétractation....24
Section 2 : Droits et obligations du professionnel....25

Section 3 : Perte du droit de rétractation et résolution ou résiliation de contrat....25
CHAPITRE V : DE LA PUBLICITE PAR VOIE ELECTRONIQUE....25
Section 1 : Des dispositions générales....25
Section 2 : Des conditions de la prospection directe....26
TITRE VIII : DES PLATEFORMES NUMÉRIQUES ET DES FOURNISSEURS EN POSITION DOMINANTE....27
TITRE IX : DE LA SURVEILLANCE, DU CONTRÔLE TECHNIQUE DES ACTIVITÉS ET SERVICES NUMÉRIQUES, DU RÈGLEMENT DES DIFFÉRENDS, DES MESURES ET SANCTIONS ADMINISTRATIVES ET DE LA PRESCRIPTION....28
CHAPITRE I : DE LA SURVEILLANCE ET DU CONTROLE TECHNIQUE DES ACTIVITES ET SERVICES NUMERIQUES....28
CHAPITRE II : REGLEMENT DES DIFFERENTS....28
CHAPITRE II : DES MESURES ET SANCTIONS ADMINISTRATIVES....29
CHAPITRE III : DE LA PRESCRIPTION....30
LIVRE II : DES ÉCRITS, DES OUTILS ÉLECTRONIQUES ET DES PRESTATAIRES DE SERVICES DE CONFIANCE....31
TITRE I : DES ÉCRITS ET OUTILS ÉLECTRONIQUES....31
CHAPITRE I : DES DISPOSITIONS GENERALES....31
CHAPITRE II : DE L'ECRIT ELECTRONIQUE....31
Section 1 : Des principes généraux....31
Section 2 : Validité de l'écrite électronique....32
Section 3 : De la preuve électronique....33
CHAPITRE III : DES OUTILS ELECTRONIQUES....35
Section 1 : De la signature électronique....35
Section 2 : Du cachet électronique....38
Section 3 : De l'horodatage électronique....39
Section 4 : De l'authentification de sites internet....39
TITRE II : DES PRESTATAIRES DE SERVICES DE CONFIANCE....40
CHAPITRE I : DES DISPOSITIONS GENERALES....40
CHAPITRE II : PRINCIPES ET CATEGORIES DES PRESTATAIRES....41
Section 1 : Des principes....41
Section 2 : Des catégories de prestataires de services de confiance....41
CHAPITRE III : OBLIGATIONS ET RESPONSABILITES....43
Section 1 : Des obligations et responsabilité des prestataires de service de confiance....43
Paragraphe 1 : Des obligations....43
Paragraphe 2 : De la responsabilité....46
Section 2 : Obligation et responsabilité du titulaire du certificat....46
Paragraphe 1 : De l'obligation....46
Paragraphe 2 : De la responsabilité....46
TITRE V : DU CONTRÔLE DES PRESTATAIRES DE SERVICES DE CONFIANCE....47
TITRE VI : DE LA CESSATION DES ACTIVITÉS....48
TITRE VII : DES SANCTIONS ADMINISTRATIVES....48
LIVRE III : DES CONTENUS NUMERIQUES....50
TITRE I : DE L'OBJET ET DU CHAMP D'APPLICATION....50
TITRE II : DES CONTENUS PUBLICS....50
CHAPITRE I : DISPOSITIONS GENERALES....50
CHAPITRE II : DE L'IDENTIFICATION ELECTRONIQUE....51

Section 1 : Des principes et des obligations....51
Section 3 : Schéma électronique....51
Section 4 : Obligations liées au moyen d'identification électronique....53
TITRE III : DES DONNÉES PERSONNELLES....54
CHAPITRE I : DISPOSITIONS GENERALES....54
CHAPITRE II : CONDITIONS DE TRAITEMENT DES DONNEES PERSONNELLES....55
CHAPITRE III : DU TRAITEMENT DES DONNEES PERSONNELLES....57
CHAPITRE IV : DE LA TRANSMISSION ET DU TRANSFERT DES DONNEES PERSONNELLES....60
Section 1 : De la transmission des données personnelles....60
Section 2 : Du transfert des données personnelles....61
CHAPITRE V : DES DONNEES PERSONNELLES SOUMISES A DES REGIMES PARTICULIERS....62
CHAPITRE VI : DES DROITS DE LA PERSONNE CONCERNEE, DES OBLIGATIONS ET DU CONTROLE DU RESPONSABLE DE TRAITEMENT, DU SOUS-TRAITANT ET DE LEUR PREPOSE DANS LE TRAITEMENT DE DONNEES PERSONNELLES....64
Section 1 : Des droits de la personne concernée....64
Section 2 : Des obligations de responsables du traitement de données personnelles....69
Section 3 : Des obligations du sous-traitant....73
Section 4 : Des obligations du préposé....74
Section 5 : Du contrôle du traitement des données personnelles....75
CHAPITRE VII : DES MESURES ADMINISTRATIVES....81
TITRE IV : DE L'AUTORITE DE PROTECTION DES DONNEES....83
LIVRE IV : DE LA SÉCURITÉ ET DE LA PROTECTION PÉNALE DES SYSTÈMES INFORMATIQUES.87
TITRE I : DE L'OBJET ET DU CHAMP D'APPLICATION....87
TITRE II : DU CADRE INSTITUTIONNEL....87
CHAPITRE I : DE L'AGENCE NATIONALE DE CYBERSECURITE....88
TITRE III : DE LA SÉCURITÉ DES SYSTÈMES INFORMATIQUES....90
CHAPITRE I : DES OBLIGATIONS GENERALES ET SPECIFIQUES....90
Section 1 : Des obligations générales....90
Section 2 : Des obligations spécifiques....92
CHAPITRE II : DE LA CRYPTOLOGIE....94
Section 1 : Des dispositions générales....94
Section 2 : Du régime juridique....94
Section 3 : Des prestataires de services de cryptologie....95
Section 4 : Des sanctions administratives....95
TITRE IV : DE LA PROTECTION PÉNALE DES SYSTÈMES INFORMATIQUES....96
CHAPITRE I : DES PRINCIPES GENERAUX....96
Section 1 : De la responsabilité pénale....96
Section 2 : Des peines....96
Section 3 : De la participation criminelle et de la tentative punissable....98
Section 4 : De la récidive et des circonstances aggravantes....98
CHAPITRE II : DES REGLES DE PROCEDURE ET DE COMPETENCE DES JURIDICTIONS....98
Section 1 : De la constatation des infractions a la législation du numérique....98
Section 2 : De la perquisition des données stockées dans un système informatique....99

Section 3 : De l'interception des données....99
Section 4 : Des poursuites....100
Section 5 : De l'extinction de l'action publique....100
Section 6 : Des juridictions compétentes....100
CHAPITRE III : DE LA QUALIFICATION DES INFRACTIONS....101
Section 1 : Des infractions de droit commun commises au moyen d'un ou sur un réseau de communication électronique ou un système informatique....101
Section 2 : Des atteintes aux systèmes informatiques....101
Paragraphe 1 : De l'accès et du maintien illégal....101
Paragraphe 2 : Des atteintes aux données d'un système informatique....102
Paragraphe 3 : Des atteintes à l'intégrité du système informatique....102
Paragraphe 4 : Des abus de dispositifs....103
Paragraphe 5 : De la falsification des données ou faux en informatique....103
Paragraphe 6 : De la fraude informatiques....104
Section 3 : Des atteintes dans le domaine de l'Agence Nationale de Cybersécurité....104
Section 4 : Des infractions liées à l'utilisation des données à caractère personnel....105
Paragraphe 1 : De l'envoi de messages non sollicités....105
Paragraphe 2 : De la tromperie....105
Paragraphe 3 : Du traitement non autorisé....105
Paragraphe 4 : De l'usurpation d'identité....106
Section 5 : De la fraude aux cartes bancaires et des infractions relatives à la publicité sur internet....106
Paragraphe 1 : De la fraude aux cartes bancaires....106
Paragraphe 2 : Des infractions relatives a la publicité sur Internet....107
Section 6 : Des contenus abusifs....107
Paragraphe 1 : De la diffusion du contenu tribaliste, raciste et xénophobe par le biais d'un système électronique....107
Paragraphe 2 : De la pornographie infantile....107
Paragraphe 3 : Du harcèlement par le biais d'une communication électronique....107
Paragraphe 4 : De la négation, minimisation grossière, approbation ou justification des crimes internationaux ou des violences sexuelles....108
Paragraphe 5 : De l'incitation ou provocation à la commission d'actes terroristes et apologie des actes terroristes....108
Paragraphe 6 : Du courrier indésirable ou pourriel ou ou spam....108
Section 7 : Des infractions à charge du fournisseur d'accès à internet....109
Section 8 : Des infractions de presse en ligne et de la divulgation des détails d'une enquête....109
Paragraphe 1 : Des infractions de presse par le biais d'une communication électronique et droit de réponse....109
Paragraphe 2 : De la divulgation des détails d'une enquête....110
Section 9 : Du cyberespionnage....110
Section 10 : De l'enregistrement des images relatives à la commission des infractions et de la diffusion des éléments pour fabriquer des engins de destruction....111
Paragraphe 1 : De l'enregistrement des images relatives à la commission des infractions....111
Paragraphe 2 : De la diffusion des éléments pour fabriquer des engins de destruction....111
Paragraphe 3 : De l'omission d'entretenir les dispositifs de protection d'un système informatique....111
Section 11 : De l'atteinte aux droits d'auteur et a la propriété intellectuelle et industrielle ainsi qu'aux droits voisins....111

Paragraphe 1 : De la contrefaçon de marque, nom commercial, appellation d'origine, indication géographique, logiciel et matériel de conception préparatoire....112
Paragraphe 2 : De la contrefaçon de dessins et modèles....112
Paragraphe 3 : De l'atteinte aux droits de propriété des brevets....112
Paragraphe 4 : De l'atteinte aux schémas de configuration d'un système numérique protégé....112
Paragraphe 5 : De l'atteinte a une mesure technique efficace....112
Paragraphe 6 : De la suppression d'un élément d'information sur le régime des droits pour porter atteinte au droit d'auteur....113

LIVRE V : DES DISPOSITIONS DIVERSES, TRANSITOIRES, ABROGATOIRES ET FINALES....114
CHAPITRE I : DU REGIME FISCAL, PARAFISCAL, DOUANIER ET DE CHANGER....114
CHAPITRE II : DE LA COMMANDE PUBLIQUE....115
CHAPITRE III : DES DISPOSITIONS TRANSITOIRES, ABROGATOIRES ET FINALES..115