REPUBLIQUE DU BURUNDI

CABINET DU PRESIDENT

LOI N°1/ 10 DU 16 MARS 2022 PORTANT PREVENTION ET REPRESSION DE LA CYBERCRIMINALITE AU BURUNDI

LE PRESIDENT DE LA REPUBLIQUE,

Vu la Constitution de la République du Burundi ;

Vu la Loi Organique n°1/27 du 9 décembre 2021 portant Modification de la Loi Organique n°1/03 du 20 février 2017 portant Missions, Organisation, Composition et Fonctionnement de la Police Nationale du Burundi ;

Vu la Loi n°1/08 du 17 mars 2005 portant Code de l'Organisation et de la Compétence Judiciaires ;

Vu la Loi n°1/08 du 30 juin 2007 portant Ratification par la République du Burundi du Traité d'Adhésion du Burundi à la Communauté Est-Africaine ;

Vu la Loi n°1/02 du 4 février 2008 portant Lutte contre le Blanchiment de Capitaux et le Financement du Terrorisme ;

Vu la Loi n°1/03 du 02 avril 2012 portant Ratification par la République du Burundi de la Convention des Nations Unies contre la Criminalité Transnationale Organisée ;

Vu la Loi n°1/28 du 29 octobre 2014 portant Prévention et Répression de la Traite des Personnes et Protection des Victimes de la Traite ;

Vu la Loi n°1/27 du 29 décembre 2017 portant Révision du Code Pénal ;

Vu la Loi n°1/09 du 11 mai 2018 portant Code de Procédure Pénale ;

Vu le Décret-loi n°1/029 du 28 juillet 1989 portant Ratification de la Convention sur la Charte Africaine des Droits de l'Homme et des Peuples ;

Vu le Décret-loi n°1/009 du 14 mars 1990 portant Ratification du Pacte International relatif aux Droits Civils et Politiques ;

Vu le Décret-loi n°1/032 du 16 août 1990 portant Ratification de la Convention relative aux Droits de l'Enfant ;

Vu le Décret-loi n°1/11 du 4 septembre 1997 portant Dispositions Organiques sur les Télécommunications ;

Le Conseil des Ministres ayant délibéré ;

L'Assemblée Nationale et le Sénat ayant adopté ;

PROMULGUE :

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

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

Article 1 : La présente loi a pour objet la prévention et la répression de toutes les infractions cybernétiques, qui sont commises au Burundi ou à l'extérieur du Burundi si ces infractions ont produit leurs effets au Burundi, ainsi que toutes les infractions pénales dont la constatation requiert la collecte d'une preuve électronique.

Elle concerne également l'accès ou la complicité pour entraver, fausser, supprimer ou modifier le fonctionnement d'un système informatique d'une infrastructure critique.

Section 2 : Des définitions

Article 2 : Au sens de la présente loi, on entend par :

1° **accès illicite :** l'accès intentionnel, sans en avoir le droit, à l'ensemble ou à une partie d'un réseau de communication électronique, d'un système d'information ou d'un équipement terminal ;

2° **chiffrement :** toute technique consistant à transformer les données numériques en un format inintelligible en employant des moyens de cryptologie ;

3° **cryptologie :** la science relative à la protection et à la sécurité des informations ;

4° **cybercriminalité :** tout fait illégal commis au moyen d'un système ou d'un réseau informatique ou de tout autre réseau physique connexe ou en relation avec un système d'information ;

5° **cyberespace :** l'ensemble de données numérisées constituant un univers d'informations et un milieu de communication lié à l'interconnexion mondiale d'équipement de traitements automatisés de données numériques ;

6° **cyber-sécurité :** l'ensemble de mesures de prévention, de protection et de dissuasion d'ordre technique, organisationnel, juridique, financier, humain, procédural et autres actions permettant d'atteindre les objectifs de sécurité fixés à travers les réseaux de communications électroniques, les systèmes d'information et pour la protection de la vie privée des personnes ;

7° **communication électronique :** toute émission, transmission ou réception de signes, de signaux, d'écrits, d'images, de sons ou de vidéos par voie électromagnétique, optique ou par tout autre moyen électronique ;

8° **données à caractère personnel :** toute information de quelque nature qu'elle soit et indépendamment de son support, y compris le son et l'image relative à une personne physique identifiée ou identifiable directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, génétique, psychique, culturelle, sociale ou économique ;

9° **données informatiques :** toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction ;

10° **électromagnétique :** le résultat de la vibration couplée d'un champ électrique et d'un champ magnétique variable dans le temps ;

11° **fournisseurs des services :** toute personne physique ou morale qui fournit un ou plusieurs services aux utilisateurs d'un système de télécommunication ;

12° **information :** tout élément de connaissance susceptible d'être représenté à l'aide de conventions pour être utilisé, conservé, traité ou communiqué ;

13° **infrastructure critique :** l'infrastructure essentielle aux services vitaux pour la sûreté publique, la stabilité économique, la sécurité nationale, la stabilité internationale et pour la pérennité et la restauration du cyberespace critique ;

14° **interception illégale :** l'accès sans en avoir le droit ou l'autorisation, aux données d'un réseau de communications électroniques, d'un système d'information ou d'un équipement terminal ;

15° **gateway :** un dispositif permettant de relier deux réseaux informatiques de types différents ;

16° **phishing :** une forme d'escroquerie par mail qui consiste à prendre l'identité d'une personne physique ou morale connue et reconnue sur un e-mail pour inciter les destinataires à changer ou mettre à jour leurs coordonnées bancaires sur des pages internet imitant celles de la personne dont l'image a été utilisée pour l'escroquerie ;

17° **pornographie infantile :** toute représentation visuelle d'un comportement sexuellement explicite y compris toute photographie, film, vidéo, image que ce soit fabriquée ou produite par voie électronique, mécanique ou par tout autre moyen impliquant un mineur ;

18° **programme informatique :** l'ensemble d'instructions exécutées par l'ordinateur pour obtenir les résultats escomptés ;

19° **réseau :** toute installation ou tout ensemble d'installations de transport ou de diffusion ainsi que le cas échéant les autres moyens assurant l'acheminement de communications électroniques notamment ceux de commutation ou de routage ;

20° **spamming :** l'envoi généralement massif et non ciblé, de messages commerciaux par e-mail avec l'intention de voler, à des individus n'ayant pas donnés leur autorisation à l'émetteur pour la réception de tels messages ;

21° **système d'information :** tout dispositif isolé ou groupe de dispositifs interconnectés ou apparentés, assurant par lui-même ou par un ou plusieurs de ses éléments, conformément à un programme, un traitement automatisé de données.

CHAPITRE II : DES OBLIGATIONS

Section 1 : Des obligations des fournisseurs des services et des opérateurs des réseaux

Paragraphe 1 : Les obligations communes

Article 3 : Les opérateurs des réseaux et les fournisseurs des services ont l'obligation de garantir la sécurité des services offerts. Ils doivent mettre en place les procédés et les moyens techniques permettant de lutter contre la fraude cybernétique.

Article 4 : Les opérateurs des réseaux et les fournisseurs des services ont l'obligation de :

1° conserver les données de connexion et de trafic pendant une période minimum de dix ans ;

2° installer des mécanismes de surveillance de trafic des données de leurs réseaux ;

3° disposer d'un centre de gestion opérationnelle de leurs infrastructures critiques sur le territoire national ;

4° mettre en place un système de vidéo-surveillance dans les cybercafés.

Paragraphe 2 : Les obligations des fournisseurs des services

Article 5 : Les fournisseurs des services ont l'obligation de :

1° informer leurs clients des tendances de la cybercriminalité qui les affectent ou qui peuvent les affecter ;

2° établir une manière procédurale de signaler la cybercriminalité à leurs clients ;

3° informer leurs clients des mesures à prendre pour se protéger contre la cybercriminalité ;

4° révéler les abus à la victime concernée et aux organes chargés de la répression de la cybercriminalité.

Article 6 : Tout fournisseur des services qui connaît ou qui prend connaissance que son ordinateur, son système informatique ou son réseau de communication électronique est utilisé pour commettre une infraction prévue par la présente loi a l'obligation de :

1° signaler immédiatement l'incident aux services chargés de l'investigation et de l'instruction criminelles ;

2° conserver toute information susceptible d'aider à enquêter sur l'infraction comme l'origine, la destination, l'itinéraire, l'heure, la date, la dimension, la durée de la communication et le type de services sous-jacents.

Article 7 : Tout fournisseur des services qui prend connaissance ou qui a été mis au courant par les organes habilités, des informations ou activités illégales a l'obligation de :

1° empêcher l'accès à ces informations ;

2° suspendre ou mettre fin aux services du client ayant lancé des informations ou entrepris des activités illégales ;

3° donner des informations nécessaires aux organes ayant l'investigation ou la poursuite judiciaire dans leurs attributions.

Paragraphe 3 : Les obligations des opérateurs des réseaux

Article 8 : Les opérateurs des réseaux doivent prendre les mesures d'interconnexion de la plateforme nationale mise en place par la gateway unique ou un autre système décidé et convenu par l'autorité compétente en la matière.

Article 9 : Les opérateurs des réseaux sont notamment tenus d'informer les usagers :

1° du danger encouru en cas d'utilisation de leurs réseaux ;

2° des risques particuliers de troubles à l'ordre et à la sécurité publics ;

3° de l'existence de moyens techniques permettant d'assurer la sécurité de leurs communications.

Section 2 : Des obligations des clients et des consommateurs

Article 10 : Les clients sont tenus de coopérer avec les services habilités dans la prévention et la répression des infractions prévues par la présente loi.

Ils doivent dénoncer et rapporter dans les brefs délais tout acte à leur connaissance susceptible de porter atteinte à la cyber-sécurité.

Article 11 : Le consommateur a l'obligation de payer toutes les factures lorsqu'elles sont arrivées à leur échéance.

Article 12 : Chaque consommateur doit veiller à ce que l'utilisation ou la consommation ne constitue pas un danger pour l'environnement. Il doit protéger tous les équipements de communication ainsi que les installations se trouvant dans son voisinage.

Article 13 : Le consommateur a l'obligation de s'affirmer de manière à ce qu'il reçoive, avec les autres utilisateurs du service, un traitement équitable.

CHAPITRE III : DES INFRACTIONS CONTRE LA CONFIDENTIALITE, L'INTEGRITE ET LA DISPONIBILITE DES DONNEES ET DES SYSTEMES INFORMATIQUES

Section 1 : De l'atteinte à la confidentialité des systèmes informatiques

Article 14 : Tout fournisseur des services ou tout opérateur des réseaux, qui n'exerce pas de diligences et de compétences nécessaires pour empêcher la divulgation des données informatiques mises à la disposition d'un tiers, est puni d'une amende de dix à trente millions de francs burundais.

Article 15 : Est puni d'une amende de dix à cinquante millions de francs burundais, tout fournisseur des services ou tout opérateur des réseaux qui fournit un accès aux données d'un ordinateur ou d'un système informatique, fait transmettre ou publie ces données, fait utiliser un programme d'un ordinateur ou un système informatique d'autrui sans autorisation.

Il est puni des mêmes peines, s'il a :

1° amorcé la transmission des données ou des programmes ;

2° sélectionné le récepteur de la transmission des données ou des programmes ;

3° sélectionné ou modifié les informations contenues dans la transmission.

Section 2 : De l'accès illégal

Article 16 : Est puni d'une servitude pénale de six mois à deux ans et d'une amende de deux à cinq millions de francs burundais ou de l'une de ces peines seulement, quiconque accède frauduleusement à un système informatique.

Article 17 : Est puni d'une servitude pénale de un à trois ans et d'une amende de cinq à dix millions de francs burundais, quiconque se procure frauduleusement, pour soi-même ou pour autrui, un avantage quelconque en s'introduisant dans un système informatique.

Article 18 : Est puni d'une servitude pénale de un an à trois ans et d'une amende de dix à quinze millions de francs burundais ou de l'une de ces peines seulement, quiconque se maintient frauduleusement dans un système informatique.

Article 19 : Est puni d'une servitude pénale de deux à cinq ans et d'une amende de quinze à vingt millions de francs burundais, celui qui accède sans droit, et en violation des mesures de sécurité, à l'ensemble ou à une partie d'un réseau de communications électroniques, d'un système d'information, d'un équipement terminal, afin d'obtenir des informations ou des données en relation avec un système d'information connecté à un autre système d'information.

Article 20 : Est puni d'une servitude pénale de deux à cinq ans et d'une amende de dix à vingt millions de francs burundais, quiconque :

1° dévoile sciemment tout code d'accès ou tout autre moyen d'accéder à un programme ou à des données détenues dans un ordinateur ou un système informatique, en visant un gain illicite ;

2° accomplit tout acte illégal sachant qu'un tel acte est susceptible de dévoiler tout code d'accès ou tout autre moyen d'accéder au système informatique.

Section 3 : De l'atteinte à l'intégrité du système informatique

Article 21 : Quiconque entrave, par quelque moyen que ce soit, le fonctionnement d'un système informatique, provoque la saturation, l'attaque d'une ressource de réseau de communication électronique ou d'un système d'information dans le but de l'effondrer en empêchant la réalisation des services attendus, est puni d'une servitude pénale de dix à quinze ans et d'une amende de dix à trente millions de francs burundais.

Lorsque le système informatique attaqué est une infrastructure critique, l'auteur est puni d'une servitude pénale de quinze à vingt ans et d'une amende de cinquante à cent millions de francs burundais.

Lorsque l'attaque a été commise dans un but de commettre des actes terroristes, l'auteur est puni d'une peine de servitude pénale à perpétuité.

Article 22 : Est puni d'une servitude pénale de cinq à dix ans et d'une amende de quinze à vingt millions de francs burundais, quiconque, sans être autorisé, commet un acte qui cause directement ou indirectement une dégradation, un échec, une interruption ou une entrave à l'exploitation d'un système informatique, un refus d'accès, un dommage de tout programme ou données stockées dans le système informatique.

Section 4 : De l'atteinte à l'intégrité des données

Article 23 : Le fournisseur des services ou l'opérateur des réseaux est puni d'une amende de cent à cinq cent millions de francs burundais lorsqu'il est impossible de retrouver l'auteur d'une communication électronique pour défaut de conservation des données relatives aux abonnés.

Article 24 : Est puni d'une servitude pénale de dix à quinze ans et d'une amende de vingt à trente millions de francs burundais, quiconque :

1° introduit, supprime ou modifie les données d'un système informatique ;

2° détruit, détériore, altère, rend inaccessible ou endommage ces données ;

3° soustrait ces données pour son usage personnel ou pour les céder à un tiers, à titre onéreux ou gratuit ;

4° détruit, entrave, fausse, perturbe, interrompt le fonctionnement d'un système informatique.

Article 25 : Sont punies des peines prévues à l'article 24, les personnes qui font usage d'un logiciel trompeur ou indésirable en vue d'effectuer des opérations sur un équipement terminal d'un utilisateur sans en informer au préalable celui-ci de la nature exacte des opérations que ledit logiciel est susceptible d'endommager.

Article 26 : Est puni d'une servitude pénale de dix à quinze ans et d'une amende de trente à cinquante millions de francs burundais quiconque, à l'aide d'un logiciel potentiellement indésirable, mène l'une des opérations visées aux articles 20 et 21 pour accéder aux informations d'un système informatique afin de commettre des infractions.

Article 27 : Est puni d'une servitude pénale de dix à quinze ans et d'une amende de dix à vingt millions de francs burundais quiconque intercepte frauduleusement par des moyens techniques des données informatiques lors de leurs transmissions non publiques à destination, en provenance ou à l'intérieur d'un système informatique, y compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données informatiques.

La peine est portée au double si l'infraction est commise au préjudice de l'Etat du Burundi.

Article 28 : Quiconque, par le biais d'un système d'information ou dans un réseau de communication contrefait, falsifie une carte de retrait, une carte de crédit, fait usage en connaissance de cause d'une carte de paiement, de crédit ou de retrait contrefaite ou falsifiée, est puni d'une servitude pénale de quinze à vingt ans et d'une amende de cinquante à cent millions de francs burundais.

Article 29 : Est puni d'une servitude pénale de cinq à dix ans et d'une amende de dix à quinze millions de francs burundais ou de l'une de ces peines seulement, quiconque reproduit, extrait ou copie intentionnellement et sans droit des données informatiques appartenant à autrui.

Article 30 : Est puni d'une servitude pénale de cinq à dix ans et d'une amende de vingt à cinquante millions de francs burundais, quiconque accède, prend frauduleusement connaissance, retarde l'accès ou supprime les communications électroniques adressées à autrui.

Est puni des mêmes peines prévues à l'alinéa précédent, celui qui intercepte sans autorisation, détourne, utilise ou divulgue les communications électroniques émises ou reçues par des voies électroniques ou procède à l'installation d'appareils conçus pour réaliser de telles interceptions.

Article 31 : Est puni d'une servitude pénale de quinze à vingt ans et d'une amende de cinquante à cent millions de francs burundais, quiconque intentionnellement rassemble, obtient, vend, achète, possède, met à la disposition, annonce ou utilise illégalement des logiciels malveillants aux fins de causer des dommages à des données, à un système informatique, à un réseau informatique, à une base de données et à un réseau de communications électroniques.

L'auteur est puni d'une servitude pénale à perpétuité si les faits prévus à l'alinéa premier portent sur une infrastructure critique ou ont causé des pertes en vies humaines.

Section 5 : De la fabrication, de la vente, de l'achat, de l'utilisation, de l'importation, de la distribution, de la possession illégale d'un système informatique et de l'incitation au suicide

Article 32 : Toute personne qui fabrique, vend, achète, utilise, importe, distribue ou possède un ordinateur ou un système informatique, rend disponible les données, les programmes ou le système informatique, les possède avec l'intention de les utiliser pour lui ou les met à la disposition d'autrui dans le but de commettre des infractions, est punie d'une servitude pénale de dix à vingt ans et d'une amende de vingt à cinquante millions de francs burundais.

Article 33 : Quiconque diffuse ou met à la disposition d'autrui par le biais d'un système informatique, un mode d'emploi, des informations, ou des procédés d'incitation au suicide, est puni d'une servitude pénale de cinq à dix ans et d'une amende de vingt à trente millions de francs burundais.

Section 6 : De la fraude informatique

Paragraphe 1 : L'escroquerie dans les systèmes informatiques

Article 34 : Est puni d'une servitude pénale de cinq à dix ans et d'une amende de dix à vingt millions de francs burundais ou de l'une de ces peines seulement, quiconque, intentionnellement et sans droit, par des manœuvres frauduleuses quelconques, à l'aide d'un moyen de communication électronique, se fait remettre ou délivrer des fonds, des meubles, des obligations, des dispositions, des billets, des promesses, des quittances, des décharges, tout ou une partie de la fortune d'autrui.

Lorsque l'infraction est commise par un fonctionnaire ou un agent de l'autorité publique en portant un uniforme, un insigne, ou en alléguant un faux ordre de l'autorité publique, la peine est portée de dix à quinze ans et à une amende de vingt à trente millions de francs burundais.

Paragraphe 2 : L'usurpation d'identité numérique

Article 35 : Est puni d'une servitude pénale de deux à cinq ans et d'une amende de dix à vingt millions de francs burundais, quiconque usurpe l'identité numérique d'un tiers ou fait usage d'une ou de plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou porter atteinte à son honneur, à sa vie privée, à son patrimoine ou à celui d'un tiers pour tirer profit ou induire en erreur d'autres personnes.

Les peines prévues à l'alinéa précédent sont portées au double si l'usurpation d'identité porte sur la personne du Chef de l'Etat.

Paragraphe 3 : Le Phishing

Article 36 : Est puni d'une servitude pénale de cinq à dix ans et d'une amende de dix à trente millions de francs burundais, quiconque établit, utilise un site web ou envoie un message électronique à l'aide d'un système informatique, avec l'intention d'obtenir des informations confidentielles du visiteur du site ou du destinataire du message pour s'en servir à des fins criminelles.

Paragraphe 4 : L'abus de confiance portant sur les données informatiques

Article 37 : Est puni d'une servitude pénale de deux à cinq ans et d'une amende de cinq à dix millions de francs burundais ou de l'une de ces peines seulement, quiconque détourne ou dissipe des données informatiques qui lui auront été remises à titre quelconque, à charge de les restituer ou d'en faire un usage déterminé.

Paragraphe 5 : Le recel des données informatiques

Article 38 : Est puni d'une servitude pénale de deux à cinq ans et d'une amende de deux à cinq millions de francs burundais ou de l'une de ces peines seulement, quiconque détient sciemment, à un titre quelconque, des données informatiques obtenues à l'aide d'une infraction.

Paragraphe 6 : L'extorsion des données informatiques

Article 39 : Est puni d'une servitude pénale de cinq à dix ans et d'une amende de dix à vingt millions de francs burundais quiconque se fait remettre par force, violence ou contrainte, des données informatiques.

Article 40 : Quiconque, à l'aide de menace écrite ou verbale de révélation ou d'imputation diffamatoire, extorque des données informatiques est puni d'une servitude pénale de deux à cinq ans et d'une amende de cinq à dix millions de francs burundais.

Paragraphe 7 : Le spamming

Article 41 : Est punie d'une servitude pénale de trois mois à un an et d'une amende de cinquante à cent mille francs burundais, toute personne qui, intentionnellement et sans autorisation :

1° envoie des messages non sollicités à plusieurs reprises à une personne ou à un grand nombre de personnes en utilisant un ordinateur ou un système informatique ;

2° utilise un ordinateur ou un système informatique pour retransmettre un message à plusieurs personnes ou le retransmettre plusieurs fois à une personne qui n'en a pas besoin.

Section 7 : Des infractions se rapportant au contenu

Paragraphe 1 : La publication d'images pornographiques à travers un ordinateur ou un système informatique

Article 42 : Est puni d'une servitude pénale de deux à cinq ans et d'une amende de deux à cinq millions de francs burundais ou de l'une de ces peines seulement, quiconque publie ou fait publier de la pornographie par le biais d'un système informatique ou par tout autre moyen de la technologie de l'information et de la communication.

Paragraphe 2 : La publication d'informations indécentes sous forme électronique

Article 43 : Toute personne qui publie, transmet ou fait publier des messages, des images et/ou des vidéos indécents à l'aide d'un ordinateur ou d'un système informatique, est punie d'une servitude pénale de deux à cinq ans et d'une amende de deux à cinq millions de francs burundais.

Article 44 : Est puni d'une servitude pénale de dix à vingt ans et d'une amende de cinq à dix millions de francs burundais, quiconque propose, prépare ou sollicite par l'intermédiaire d'un ordinateur, d'un système informatique, de n'importe quels réseaux, des rencontres dans le but de s'engager dans des activités sexuelles avec le mineur.

Paragraphe 3 : La production, l'importation, l'exportation, la possession d'une image ou d'une représentation à caractère pornographique

Article 45 : Est puni d'une servitude pénale de cinq à dix ans et d'une amende de vingt à trente millions de francs burundais, quiconque produit, enregistre et met à disposition une image ou une représentation présentant un caractère de pornographie par le biais d'un système informatique ou par tout autre procédé technique quelconque.

Les peines sont portées au double si les images pornographiques mettent en scène un ou plusieurs enfants âgés de moins de dix-huit ans.

Article 46 : Est puni d'une servitude pénale de deux à cinq ans et d'une amende de un à deux millions de francs burundais ou de l'une de ces peines seulement, quiconque se procure ou procure pour autrui, importe ou fait importer, exporte ou fait exporter une image ou une représentation à caractère pornographique par le biais d'un système informatique ou par tout autre procédé technique quelconque.

Les peines sont portées au double si les images ou représentations portent sur des enfants âgés de moins de dix-huit ans.

Article 47 : Quiconque possède sciemment des images ou des représentations à caractère pornographique mettant en scène un ou plusieurs enfants âgés de moins de dix-huit ans, dans un système informatique ou dans un moyen quelconque de stockage des données informatisées est puni d'une servitude pénale de dix à quinze ans et d'une amende de dix à vingt millions de francs burundais.

Est punie des mêmes peines, toute personne qui sciemment, facilite l'accès à des images, à des documents, au son ou à une représentation à caractère pornographique à un mineur.

Paragraphe 4 : La consultation publique de sites pornographiques

Article 48 : Est puni d'une servitude pénale de deux à cinq ans et d'une amende de deux à cinq millions de francs burundais, quiconque intentionnellement et sans droit, consulte un service de communication en ligne mettant à disposition du public des images ou vidéos pornographiques.

La peine est portée au double si la projection des images ou vidéos pornographiques est à titre onéreux ou si la projection porte sur des images pédopornographiques.

Paragraphe 5 : Les écrits ou les images de nature raciste ou xénophobe par le biais d'un système informatique

Article 49 : Est puni d'une servitude pénale de cinq ans à dix ans et d'une amende de cinq à dix millions de francs burundais, quiconque crée, télécharge, diffuse ou met à la disposition sous quelque forme que ce soit des écrits, messages, photos, dessins, vidéos ou toute

autre représentation d'idées ou de théories de nature raciste ou xénophobe, par le biais d'un système informatique.

La peine est portée au double pour toute personne qui, par tout moyen de communication, incite à la haine et à la violence.

Paragraphe 6 : La menace, le chantage et la publication des rumeurs

Article 50 : Est puni d'une servitude pénale de deux ans à cinq et d'une amende de dix à vingt millions de francs burundais quiconque exerce une menace par le biais d'un système informatique envers une personne en raison de son appartenance à un groupe, à sa race, à sa couleur, à son ascendance, à son origine nationale ou ethnique, à sa religion dans la mesure où cette appartenance sert de prétexte à l'un ou l'autre de ces éléments.

Lorsque la menace est faite avec ordre ou sous condition d'accomplir ou laisser accomplir un acte illicite ou préjudiciable à autrui, la peine est de cinq à dix ans de servitude pénale et d'une amende de vingt à trente millions de francs burundais.

Lorsqu'il s'agit d'une menace de mort, la peine est de dix à quinze ans de servitude pénale et d'une amende de dix à vingt millions de francs burundais.

Article 51 : Est puni d'une servitude pénale de dix à quinze ans et d'une amende de quinze à vingt millions de francs burundais ou de l'une de ces peines seulement, quiconque, au moyen d'une menace, porte atteinte à la confidentialité, à l'intégrité des données informatiques ou au fonctionnement du système informatique.

Les peines prévues à l'alinéa 1 sont portées au double lorsque l'auteur a mis sa menace à exécution.

Article 52 : Quiconque, par un ordinateur ou un système informatique, publie sciemment des rumeurs pouvant provoquer la peur, le soulèvement ou la violence entre la population ou pouvant faire perdre la crédibilité d'une personne physique ou morale, est puni d'une servitude pénale de cinq à dix ans et d'une amende de cinq à dix millions de francs burundais.

Paragraphe 7 : De l'injure commise par le biais d'un système informatique

Article 53 : L'injure commise par le biais d'un système informatique envers une personne en raison de son appartenance à un groupe qui se caractérise notamment par la race, la couleur, l'ascendance, l'origine nationale ou ethnique ou la religion dans la mesure où cette appartenance sert de prétexte à l'un ou l'autre de ces éléments, ou un groupe de personnes qui se distingue par l'une de ces caractéristiques, est punie de un à deux ans de servitude pénale et d'une amende de un à trois millions de francs burundais.

CHAPITRE IV : DES INFRACTIONS LIEES AU TERRORISME, A LA FABRICATION DES ARMES, AU TRAFIC DES PERSONNES OU DE STUPEFIANTS

Article 54 : Est puni d'une servitude pénale de quinze ans à vingt ans et d'une amende de cent à cinq cent millions de francs burundais, quiconque :

1° établit, publie ou utilise un site d'un groupe terroriste à l'aide d'un système informatique afin de faciliter la communication par son leadership ou ses membres ;

2° mobilise des fonds ou diffuse ses idées ou connaissances sur la façon dont il mène ses opérations de nature terroriste à l'aide d'un système informatique.

Article 55 : Quiconque commet des actes de terrorisme visant des logiciels ou programmes informatiques est puni d'une servitude pénale à perpétuité.

Article 56 : Est puni d'une servitude de dix à vingt ans et d'une amende de cinquante à cent millions de francs burundais, quiconque diffuse ou met à la disposition d'autrui par le biais d'un système informatique, sauf à destination des personnes autorisées, un mode d'emploi ou des procédés permettant la fabrication des armes à feu, de leurs pièces, éléments et munitions de nature à porter atteinte à la vie humaine, aux biens ou à l'environnement.

Article 57 : Est puni d'une servitude pénale de dix à quinze ans et d'une amende de cinquante à cent millions de francs burundais, quiconque établit ou publie un site sur un réseau d'information, sur un matériel informatique ou sur un système informatique à des fins de traite des personnes ou qui facilite une telle transaction.

Article 58 : Est punie d'une servitude pénale de dix ans à vingt ans et d'une amende de cent millions à cent cinquante millions de francs burundais, toute personne qui crée un site ou publie sur un réseau d'information, sur un matériel informatique ou sur un système informatique pour trafic ou distribution de drogues, de stupéfiants ou facilitant une telle transaction.

CHAPITRE V : DE L'ATTEINTE A LA SURETE DE L'ETAT

Article 59 : Est coupable de trahison et est puni d'une servitude pénale à perpétuité tout burundais qui :

1° livre à une nation étrangère ou à ses agents, par voie informatique, un renseignement, un objet, un document, un procédé, une donnée ou un fichier qui doit être tenu secret dans l'intérêt de la sécurité nationale ;

2° s'assure par voie informatique la possession d'un renseignement, d'un objet, d'un document, d'un procédé, d'une donnée informatisée ou d'un fichier informatisé en vue de le livrer à une puissance étrangère ou à ses agents ;

3° détruit ou laisse détruire un renseignement, un objet, un document, un procédé, des données numérisées ou des fichiers informatisés en vue de favoriser une puissance étrangère.

Article 60 : Est puni d'une servitude pénale à perpétuité, tout burundais ou étranger qui rassemble des renseignements, des objets, des documents, des procédés, des données ou des fichiers informatisés, dans l'intention de les livrer à tout pays tiers dont la réunion et l'exploitation sont de nature à nuire à la sûreté de l'Etat.

Est puni de la même peine, tout dépositaire par état ou par profession, qui détient un renseignement, un objet, un document, un procédé, une donnée numérisée ou un fichier informatisé qui doit être tenu secret dans l'intérêt de la sûreté de l'Etat ou dont la connaissance peut conduire à la découverte d'un secret de défense nationale, qui, sans ou avec intention de trahison ou d'espionnage, l'a :

1° détruit, soustrait, laissé détruire ou soustraire, reproduit, ou fait reproduire ;

2° porté ou laissé porter à la connaissance d'une personne non qualifiée ou du public.

CHAPITRE VI : DE L'ATTEINTE A LA VIE PRIVEE

Article 61 : Est puni d'une servitude pénale de deux à cinq ans et d'une amende de trois à six millions de francs burundais, quiconque, au moyen d'un procédé électronique, porte atteinte à l'intimité de la vie privée d'autrui en fixant, en enregistrant ou en transmettant, sans le consentement de l'auteur, des données électroniques ayant un caractère privé ou confidentiel.

Sont passibles des mêmes peines, les personnes qui, sans droit, interceptent des données personnelles lors de leur transmission d'un système informatique à un autre.

Est puni des mêmes peines prévues à l'alinéa premier, celui qui intercepte sans autorisation, détourne, utilise ou divulgue les communications électroniques émises ou reçues par des voies électroniques ou procède à l'installation d'appareils conçus pour réaliser de telles interceptions.

Article 62 : Est puni d'une servitude pénale de deux à cinq ans d'une amende de cinq à dix millions de francs burundais, quiconque met ou fait mettre en ligne, conserve ou fait conserver en mémoire informatisée, sans l'accord exprès de l'intéressé, des données nominatives qui, directement ou indirectement font apparaître ses origines, ses opinions politiques, religieuses et ses appartenances syndicales ou ses mœurs.

Est puni des peines prévues à l'alinéa précédent, quiconque détourne les informations, notamment à l'occasion de leur enregistrement, de leur classement et de leur transmission.

Article 63 : Est puni d'une servitude pénale de deux à cinq ans et d'une amende de deux à cinq millions de francs burundais, quiconque, utilise de manière frauduleuse, le système automatisé de traitement des données d'une autre personne ou dans des systèmes similaires dans le but de découvrir des données stockées ou transmises électroniquement.

CHAPITRE VII : DE LA PROCEDURE EN MATIERE DE CYBERCRIMINALITE

Article 64 : Les dispositions du présent chapitre ne font pas obstacles à l'application du code de procédure pénale.

Article 65 : Lorsque, dans le cadre d'une enquête ou d'une instruction, il y a des raisons de penser que les données informatiques spécifiques, y compris des données relatives aux abonnés et au trafic stockées au moyen d'un système informatique sont susceptibles de perte ou de modification, l'autorité compétente procède ou fait procéder à la conservation immédiate desdites données.

Article 66 : S'il est avéré que des données, accessibles à partir du système initial ou disponible pour le système initial, sont stockées dans un autre système informatique situé hors du territoire national, elles sont recueillies par l'autorité compétente, sous réserve de respect des engagements internationaux.

Article 67 : L'autorité compétente peut, dans les conditions prévues par le code de procédure pénale, procéder à la saisie des systèmes informatiques, des supports de stockages informatiques ou procéder à la copie des données informatiques nécessaires à la manifestation de la vérité.

Lorsqu'une copie est réalisée dans le cadre de cette procédure, il peut être procédé, sur décision du juge, à l'effacement définitif sur le support physique qui n'a pas été placée sous main de justice, des données informatiques dont la détention ou l'usage est illégal ou dangereux pour la sécurité des personnes ou des biens.

Lorsque les systèmes informatiques ou les supports de stockage informatique sont mis sous scellés, ils ne peuvent être ouverts que selon les modalités prévues par le code de procédure pénale.

Article 68 : Sur réquisition de l'Officier du ministère public ou sur ordonnance du juge, l'Officier de Police Judiciaire est habilité :

1° à collecter ou enregistrer par tout moyen technique, les données relatives au trafic ou au contenu, associées à des communications spécifiques transmises sur son territoire au moyen d'un système informatique ;

2° à obliger un fournisseur des services, dans le cadre de ses capacités techniques existantes, à collecter ou enregistrer par tout moyen technique ou à prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer en temps réel, les données relatives au trafic ou au contenu, associées à des communications spécifiques transmises sur son territoire au moyen d'un système d'information.

CHAPITRE VIII : DES DISPOSITIONS FINALES

Article 69 : Toutes dispositions antérieures contraires à la présente loi sont abrogées.

Article 70 : La présente loi entre en vigueur le jour de sa promulgation.

Fait à Gitega, le 16 mars 2022

Evariste NDAYISHIMIYE.-

PAR LE PRESIDENT DE LA REPUBLIQUE,

VU ET SCELLE DU SCEAU DE LA REPUBLIQUE,

LE MINISTRE DE LA JUSTICE,

Domine BANYANKIMBONA.