

Loi

Générale

modern

Loi n° 66/AN/14/7ème L relative au cyber sécurité et à la lutte contre la cybercriminalité.

n° 66/AN/14/7ème L

Ministère
ASSEMBLÉE NATIONALE

Date de publication
20 juillet 2014

Numéro JO
n° 1 du 31/07/2014

Date du numéro
31 juillet 2014

INTRODUCTION

L'ASSEMBLÉE NATIONALE A ADOPTÉ LE PRÉSIDENT DE LA RÉPUBLIQUE PROMULGUÉ LA LOI DONT LA TENEUR SUIT :

VISAS

VU La Constitution du 15 septembre 1992

VU La Loi Constitutionnelle n°92/AN/10/6ème L du 21 avril 2010 portant révision de la Constitution

VU La Loi n°178/AN/12/6ème L du 17 octobre 2012 relative aux attributions et à l'organisation du Ministère de la Justice

VU Le Code pénal djiboutien de 1995 notamment en ses articles 441 à 445 et de 548 à 555

VU Le Décret n°2013-044/PRE du 31 mars 2013 portant nomination Premier Ministre

VU Le Décret n°2013-045/PRE du 31 mars 2013 portant nomination des membres du Gouvernement

VU Le Décret n°2013-058/PRE du 14 avril 2013 fixant les attributions des Ministères

VU La Circulaire n°147/PAN du 10 juillet 2014 convoquant l'Assemblée nationale en sa 2ème séance publique de la Session Extraordinaire

Le Conseil des Ministres entendu en sa séance du 22 avril 2014.

TEXTE INTÉGRAL

SOMMAIRE TITRE I : DES INFRACTIONS LIÉES AUX TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION-

Chapitre préliminaire : Article (1 et 2) Chapitre premier : atteintes aux systèmes informatiques Section première : atteintes à la confidentialité des systèmes informatiques Article 1.1.1 et

Article 1

1.2 Section II : atteintes à l'intégrité des systèmes informatiques Article 1.2.1 Section III : atteintes à la disponibilité des systèmes informatiques Article 1.3.1 Chapitre II : atteintes aux données informatisées Section première : atteintes générales aux données informatiques Articles (2.1.1 – 2.1.2 – 2.1.3 – 2.1.4 – 2.1.5)

Chapitre III : des autres formes d'abus Articles : (3.1 – 3.2)

Chapitre IV : infraction se rapportant au contenuSection première : pornographie infantileArticles : (4.1.1 – 4.1.2 – 4.1.3 – 4.1.4)Section II : autres atteintes se rapportant au contenuArticles : (4.2.1 – 4.2.2 – 4.2.3 – 4.2.4 – 4.2.5)

Chapitre V : responsabilité pénale des personnes moralesArticles (5.1 à 5.3)TITRE II : DE LA PROCEDURE EN MATIERE D'INFRACTIONS COMMISES AU MOYEN DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATIONChapitre I : de la perquisition et de la saisie(

Articles 1

1 et 1.2)

Chapitre II : de la conservation rapide de données informatisées archivées(

Article 2

1)

Chapitre III : interception des données informatiséesArticles (3.1 – 3.2)Disposition transitoireArticle 3.3TITRE I : DES INFRACTIONS LIEES AUX TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATIONChapitre préliminaire : Article premier : Les dispositions de la présente loi viennent compléter les articles 441 à 445 sur les atteintes aux droits de la personne résultant des traitements informatiques et les articles 548 à 555 traitant des infractions en matière informatique, du code pénal.Article deuxième : DéfinitionsAu sens de la présente loi, on entend par :1. Cybercriminalité : toutes les infractions pénales susceptibles de se commettre sur ou au moyen d'un système informatique généralement connecté à un réseau

- 2 Communication électronique : toute mise à la disposition au public ou d'une catégorie de public, par un procédé de communication électronique ou magnétique, de signes, de signaux, d'écrits, d'images, de sons ou de messages de toute nature
- 3 Données informatisées : toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique
- 4 Raciste et xénophobe en matière des technologies de l'information et de la communication : tout écrit, toute image ou toute autre représentation d'idées ou de théories qui préconise ou encourage la haine, la discrimination ou la violence contre une personne ou un groupe de personnes, en raison de la race, de la couleur, de l'ascendance ou de l'origine nationale ou ethnique ou de la religion, dans la mesure où cette dernière sert de prétexte à l'un ou l'autre de ces éléments ou qui incite à de tels actes ;5. Mineur : toute personne âgée de moins de 18 ans au sens de la convention des Nations Unies sur les droits de l'enfant
- 6 Pornographie infantile : toute donnée quelle qu'en soit la nature ou la forme représentant de manière visuelle un mineur se livrant à un agissement sexuellement explicite ou des images réalistes représentant un mineur se livrant à un comportement sexuellement explicite
- 7 Système informatique : tout dispositif isolé ou non, tout ensemble de dispositifs interconnectés assurant en tout ou partie, un traitement automatisé de données en exécution d'un programme
- 8 Données à caractère personnel : toute information relative à une personne physique identifiée ou identifiable directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments, propres à son identité physique, physiologique, génétique, psychique, culturelle, sociale ou économique.CHAPITRE PREMIER : ATTEINTES AUX SYSTEMES INFORMATIQUESSECTION PREMIERE : ATTEINTES A LA CONFIDENTIALITE DES SYSTEMES INFORMATIQUESArticle 1.1.1 : Quiconque aura accédé ou tenté d'accéder frauduleusement à tout ou partie d'un système informatique, sera puni d'un emprisonnement de trois (3) ans et d'une amende 10.000.000 francs ou de l'une de ces deux peines seulement. Est puni des mêmes peines, celui qui se procure ou tente de se procurer frauduleusement, pour soi-même ou pour autrui, un avantage quelconque en s'introduisant dans un système informatique.

Article 1

1.2 : Quiconque se sera maintenu ou aura tenté de se maintenir frauduleusement dans tout ou partie d'un système informatique, sera puni d'un emprisonnement de trois (3) ans et d'une amende de 10.000.000 francs ou de l'une de ces deux peines seulement.

SECTION II : ATTEINTES A L'INTEGRITE DES SYSTEMES INFORMATIQUES Article 1.2.1 : Quiconque aura accédé ou tenté d'accéder frauduleusement, introduit ou tenté d'introduire frauduleusement des données dans un système informatique, sera puni d'un emprisonnement de cinq (5) ans et d'une amende de 25.000.000 francs ou de l'une des ces deux peines seulement.

SECTION 3 : ATTEINTES A LA DISPONIBILITE DES SYSTEMES INFORMATIQUES Article 1.3.1 : Quiconque aura troublé ou altéré ou aura tenté de troubler ou d'altérer le fonctionnement d'un système informatique sera puni d'un emprisonnement de cinq (5) ans et d'un amende de 25.000.000 francs ou de l'une de ces deux peines seulement.

CHAPITRE II : ATTEINTES AUX DONNEES INFORMATISEES SECTION PREMIERE : ATTEINTES GENERALES AUX DONNEES INFORMATISEES Article 2.1.1 : Quiconque aura intercepté ou tenté d'intercepter frauduleusement par des moyens techniques des données informatisées lors de leur transmission non publique à destination, en provenance ou à l'intérieur d'un système informatique, sera d'un emprisonnement de cinq (5) ans et d'une amende de 25.000.000 francs ou de l'une de ces deux peines seulement.

Article 2

1.2 : Quiconque aura endommagé ou tenté d'endommager, effacé ou tenté d'effacer, détérioré ou tenté de détériorer, altéré ou tenté d'altérer, modifié ou tenté de modifier, frauduleusement des données informatisées, sera puni d'un emprisonnement de cinq (5) ans et d'une amende de 25.000.000 francs ou de l'une de ces deux peines seulement.

Article 2

1.3 : Quiconque aura produit ou fabriqué un ensemble de données numérisées par l'introduction, l'effacement ou la suppression frauduleuse de données informatisées stockées, traitées ou transmises par un système informatique, engendrant des données contrefaites, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient originales, sera puni d'un emprisonnement de cinq (5) ans et d'une amende de 25.000.000 francs ou de l'une de ces deux peines seulement.

Article 2

1.4 : Est puni des mêmes peines celui qui, en connaissance de cause, aura fait usage ou tenté de faire usage des données obtenues dans les conditions prévues à l'

article 2

1.3 de la présente loi.

Article 2

1.5 : Quiconque aura obtenu frauduleusement, pour soi-même ou pour autrui, un avantage quelconque, par l'introduction, l'altération, l'effacement ou la suppression de données informatisées ou par toute forme d'atteinte au fonctionnement d'un système informatique, sera puni d'un emprisonnement de cinq (5) ans et d'une amende de 25.000.000 francs ou de l'une de ces deux peines seulement.

CHAPITRE III : DES AUTRES FORMES D'ABUS Article 3.1 : Quiconque aura produit, vendu, importé, détenu, diffusé, offert, cédé ou mis à disposition un équipement, un programme informatique, tout dispositif ou donnée conçue ou spécialement adaptée pour commettre une ou plusieurs des infractions prévues par les

articles 1

2.1 à 2.1.4 de la présente loi ou un mot de passe, un code d'accès ou des données informatisées similaires permettant d'accéder à tout ou partie d'un système informatique, sera puni d'un emprisonnement de 5 ans et d'une amende de 25.000.000 FD.

Article 3

2 : Quiconque aura participé à une association formée ou à une entente établie en vue de préparer ou de commettre une ou plusieurs des infractions prévues par la présente loi, sera puni d'un emprisonnement de 10 ans et d'une amende de 25.000.000 FD.

CHAPITRE IV : INFRACTION SE RAPPORTANT AU CONTENU SECTION PREMIERE : PORNOGRAPHIE INFANTILE Article

4.1.1 : Quiconque aura produit, enregistré, offert, mis à disposition, diffusé, transmis une image ou une représentation présentant un caractère de pornographie infantile par le biais d'un système informatique, sera puni d'un emprisonnement de dix (10) ans et d'une amende de 25.000.000 francs ou de l'une de ces deux peines seulement.

Article 4

1.2 : Quiconque se sera procuré ou aura procuré à autrui, importé ou fait importer, exporté ou fait exporter une image ou une représentation présentant un caractère de pornographie infantile par le biais d'un système informatique, sera puni d'un emprisonnement de dix (10) ans et d'une amende de 25.000.000 francs ou de l'une de ces deux peines seulement.

Article 4

1.3 : Sera puni des mêmes peines, celui qui possède une image ou une représentation présentant un caractère de pornographie infantile dans un système informatique ou dans un moyen quelconque de stockage de données informatisées. Sera puni des mêmes peines, quiconque aura facilité l'accès à des images, des documents, du son ou une représentation présentant un caractère de pornographie à un mineur.

Article 4

1.4 : Les infractions prévues par la présente loi, lorsqu'elles ont été commises en bande organisée, seront punies de 10 ans d'emprisonnement et de 25.000.000 FDJ. SECTION II : AUTRES ATTEINTES SE RAPPORTANT AU CONTENU Article 4.2.1 : Quiconque aura créé, téléchargé, diffusé ou mis à disposition sous quelque forme que ce soit des écrits, messages, photos, dessins ou toute autre représentation d'idées ou de théories, de nature raciste ou xénophobe, par le biais d'un système informatique sera puni d'un emprisonnement de (5) ans et d'une amende de 25.000.000 francs.

Article 4

2.2 : La menace commise par le biais d'un système informatique, de commettre une infraction pénale, envers une personne en raison de son appartenance à un groupe qui se caractérise par la race, la couleur, l'ascendance ou 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 une de ces caractéristiques sera puni d'un emprisonnement de dix (10) ans et d'une amende 25.000.000 francs.

Article 4

2.3 : L'injure commise par le biais d'un système informatique envers une personne en raison de son appartenance à un groupe qui se caractérise par la race, la couleur, l'ascendance ou 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 une de ces caractéristiques sera puni d'un emprisonnement de (10) ans et d'une amende de 25.000.000 francs.

Article 4

2.4 : Quiconque aura intentionnellement nié, approuvé ou justifié des actes constitutifs de génocide ou de crimes contre l'humanité par le biais d'un système informatique, sera puni d'un emprisonnement de (10) ans et d'une amende de 25.000.000 francs.

Article 4

2.5 : En cas de condamnation, le tribunal pourra prononcer la confiscation des matériels équipements, instruments, programmes informatiques ou tous dispositifs ou données appartenant au condamné et ayant servi à commettre les infractions prévues aux

articles 1

2.1 à 4.2.4 de la présente loi.

CHAPITRE V : RESPONSABILITE PENALE DES PERSONNES MORALES Article 5.1 : Les personnes morales autres que l'Etat, les collectivités publiques et les établissements publics sont pénalement responsables des infractions prévues par la présente loi, commises pour leur compte par leurs organes ou représentants. La responsabilité des personnes morale n'exclut pas celle des personnes physiques auteurs, instigateurs ou complices des mêmes faits. Les peines encourues par les personnes morales sont : 1) L'amende dont le taux maximum est égal au quintuple de celui prévu pour les personnes physiques par la loi qui réprime l'infraction ; 2) La dissolution, lorsque la personne morale a été créée ; 3) L'interdiction à titre définitif ou pour une durée de cinq (5) ans au plus d'exercer directement ou indirectement une ou plusieurs activités professionnelles ou sociales ; 4) La fermeture définitive ou pour une durée de cinq (5) ans au plus d'un ou plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ; 5) L'exclusion des marchés publics à titre définitif ou pour une durée de cinq (5) ans au plus ; 6) L'interdiction à titre définitif ou pour une durée de cinq (5) ans au plus de faire appel public à l'épargne ; 7) L'interdiction pour une durée de cinq (5) ans au plus d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés ou d'utiliser des cartes de paiement ; 8) La confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit ; 9) L'affichage de la décision prononcée ou la diffusion de celle-ci soit par la presse écrite soit par tout moyen de communication au public par voie électronique.

Article 5

2 : S'il y a condamnation pour une infraction commise par le biais d'un support de communication numérique, la juridiction peut prononcer à titre de peines complémentaires l'interdiction d'émettre des messages de communication numérique, l'interdiction à titre provisoire ou définitif de l'accès au site ayant servi à commettre l'infraction. Le juge peut ordonner à toute personne responsable légalement du site ayant servi à commettre l'infraction, à toute personne qualifiée de mettre en oeuvre les moyens techniques nécessaires en vue de garantir, l'interdiction d'accès, d'hébergement ou la coupure de l'accès au site incriminé. La violation des interdictions prononcées par le juge sera punie d'un emprisonnement de cinq ans d'emprisonnement et d'une amende de 25.000.000 francs.

Article 5

3 : En cas de condamnation à une infraction commise par le biais d'un support de communication numérique, le juge ordonne à titre complémentaire la diffusion au frais du condamné, par extrait, de la décision sur ce même support. La publication prévue à l'alinéa précédent doit être exécutée dans les 15 jours suivant le jour où la condamnation est devenue définitive. Le condamné qui ne fera pas diffuser ou qui ne diffusera pas l'extrait prévu à l'alinéa précédent sera puni des peines prévues par l'

article 5

2. TITRE II : DE LA PROCEDURE EN MATIERE D'INFRACTIONS COMMISES AU MOYEN DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION CHAPITRE I : DE LA PERQUISITION ET DE LA SAISIE Article 1.1 : Lorsque des données stockées dans un système informatique ou dans un support permettant de conserver des données informatisées sur le territoire djiboutien, sont utiles à la manifestation de la vérité, le juge d'instruction peut opérer une perquisition ou accéder à un système informatique ou à une partie de celui-ci ou dans un autre système informatique, 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 le juge d'instruction, par voie de commission rogatoire internationale.

Article 1

2 : Lorsque le juge d'instruction découvre dans un système informatique des données stockées qui sont utiles pour la manifestation de la vérité, mais que la saisie du support ne paraît pas souhaitable, ces données, de même que celles qui sont nécessaires pour les comprendre, sont copiées sur des supports de stockage informatique pouvant être saisis et placés sous scellés.

CHAPITRE II : DE LA CONSERVATION RAPIDE DE DONNEES INFORMATISEES ARCHIVEES

Article 2.1 : Si les nécessités de l'information l'exigent, notamment lorsqu'il y a des raisons de penser que des données informatisées archivées dans un système informatique sont particulièrement susceptibles de perte ou de modification, le juge d'instruction peut faire injonction à toute personne de conserver et de protéger l'intégrité des données en sa possession ou sous son contrôle, pendant une durée de deux ans maximum, pour la bonne marche des investigations judiciaires. Le gardien des données ou toute autre personne chargée de conserver celles-ci est tenu d'en garder le secret. Toute violation du secret est punie des peines applicables au délit de violation du secret professionnel.

CHAPITRE III : INTERCEPTION DES DONNEES INFORMATISEES

Article 3.1 : Si les nécessités de l'information l'exigent, le juge d'instruction peut ordonner à toute autorité compétente de collecter ou enregistrer en temps réel, les données relatives au contenu de communication spécifiques, transmises au moyen d'un système informatique ou obliger un fournisseur de services, dans le cadre de ses capacités techniques à collecter ou à enregistrer, ou à prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer lesdites données informatisées. Le fournisseur d'accès est tenu de garder le secret. Toute violation du secret est punie des peines applicables au délit de violation du secret professionnel.

Article 3

2 : L'officier de police judiciaire peut, pour les nécessités de l'enquête ou de l'exécution d'une délégation judiciaire, procéder aux opérations prévues par les

articles 1

1 à 3.1. Disposition transitoire Article 3.3 : La présente Loi sera publiée dès sa promulgation au Journal Officiel de la République de Djibouti.

*Le Président de la République
chef du Gouvernement*

ISMAÏL OMAR GUELLEH