BURKINA FASO

UNITE- PROGRES - JUSTICE

ASSEMBLEE NATIONALE

IV REPUBLIQUE

SEPTIEME LEGISLATURE

AVANT-PROJET DE LOI N°...-2016/AN DU ……..2017 PORTANT PROMOTION DE LA CYBERSECURITE ET LUTTE CONTRE LA CYBERCRIMINALITE

L'ASSEMBLEE NATIONALE

VU la Constitution ;

VU la résolution N° 001-2015/AN du 30 décembre 2015 portant validation du mandat des députés ;

a délibéré en sa séance du……..
et adopté la loi dont la teneur suit :

Table des matières

Exposé des motifs

Dans la perspective du programme présidentiel, « ensemble, le progrès est possible », les télécommunications, les TIC et le numérique sont appelés à constituer des leviers essentiels du développement socio-économique du Burkina-Faso. Les autorités politiques se sont alors résolument engagées à œuvrer pour le développement de l'Economie numérique et l'édification d'une société de l'information sécurisée, inclusive, ouverte et solidaire. Le contexte actuel laisse déjà apparaître, avec le développement progressif de l'ère du numérique à l'échelle planétaire mais aussi au Burkina Faso, une dépendance croissante de tous les secteurs d'activités humaines aux technologies de l'information et de la communication (TIC). Cette montée en puissance de la transformation digitale et de la dépendance technologique qu'elle induit s'explique par le fait que les réseaux numériques et les ressources innombrables qu'ils recèlent constituent aujourd'hui des porteurs de puissants moyens d'évolution de la société humaine que le Burkina Faso entend pleinement capitaliser.

La réussite du développement de l'Economie numérique et de l'édification d'une société de l'information est toutefois fortement tributaire d'un environnement juridique et institutionnel de confiance qui promeut une culture de la cybersécurité fortement ancrée dans les mentalités des citoyens et qui fonde l'intervention des institutions publiques et des divers acteurs socio-économiques. Il est en effet primordial pour notre pays de prendre conscience de la gravité de toutes les nouvelles formes de menaces et risques numériques divers qui accompagnent la civilisation numérique. Les menaces et risques technologiques ont fini aujourd'hui par dévoiler la vulnérabilité et la fragilité de l'ordre politico-institutionnel établi, des infrastructures essentielles ou d'importance vitale, mais aussi des systèmes de défense et de sécurité. Les systèmes d'information, parce qu'ils reposent sur des architectures en réseaux, constituent des ressources accessibles à distance. Ils deviennent ainsi des cibles potentielles des cyberattaques, se manifestant notamment par des atteintes à la capacité à traiter, sauvegarder, communiquer le capital informationnel, aux valeurs immatérielles et aux symboles, aux processus de production ou de décision etc. Les conséquences des cyberattaques se particularisent par leur caractère dévastateur notamment sur la sécurité des individus, la pérennité et la stabilité des Etats et des organisations publiques comme privées. Tels des « cavaliers apocalyptiques », les cybermenaces, qui se dressent comme des défis à l'humanité et à ses mécanismes de gouvernance, sont aujourd'hui en nette progression. Elles se dressent également comme l'un des obstacles majeurs à la construction d'une Economie numérique compétitive et durable pour notre nation, mais aussi pour une société burkinabè de l'information sûre.

L'audit de l'environnement juridique et institutionnel global des TIC du Burkina Faso a mis en évidence l'inexistence de mécanismes juridiques de promotion d'une culture nationale de la cybersécurité. Il aussi a révélé une inadaptation de notre dispositif pénal à prendre en charge

la spécificité du phénomène cybercriminel marqué notamment par sa transnationalité, son immatérialité, sa volatilité, mais aussi par l'anonymat de ses acteurs.

Au plan régional, les Etats membres de l'Union Africaine ont pris conscience de l'importance des enjeux et défis sécuritaires que pose l'ère du numérique. Ils ont ainsi adopté, lors de sa 23e session tenue le 27 juin 2014 à Malabo en Guinée équatoriale, la Convention de l'Union Africaine sur la cybersécurité et la protection des données à caractère personnel. Cette initiative de l'Union Africaine complète ainsi et renforce le dispositif juridique déjà mis en place au plan communautaire et composé notamment de la Directive C/DIR/1/08/11 du 19 août 2011 portant lutte contre la cybercriminalité dans l'espace de la CEDEAO. Le Burkina Faso tarde, depuis l'adoption de la Directive CEDEAO, à procéder à la transposition de ses dispositions et à combler son vide juridique et institutionnel en matière de lutte contre la cybercriminalité. Aujourd'hui, l'adoption de la Convention de Malabo doit être saisie comme une opportunité de mettre à niveaux notre dispositif juridique et institutionnel de promotion de la cybersécurité et de lutte contre la cybercriminalité. Il s'agit par la même occasion de rendre effectif la transposition de la Directive C/DIR/1/08/11 de la CEDEAO portant lutte contre la cybercriminalité.

L'objet du présent projet de loi est de doter le Burkina Faso d'un arsenal juridique et institutionnel rénové et réadapté qui soit en mesure d'assurer l'instauration effective de mécanismes adéquats de promotion de la cybersécurité sur toute l'étendue du territoire. Il vise également une adaptation du système pénal national, par la modernisation des incriminations du droit pénal classique et d'un réaménagement des règles de procédure pénale, au regard des exigences de l'environnement numérique.

Le présent projet de loi prévoit ainsi une modification du Code pénal et du Code de procédure pénale. Il est structuré autour de quatre grands titres qui se présentent comme suite :

- Le Titre I est consacré aux dispositions générales ;
- Le Titre II définit les mécanismes de promotion de la cybersécurité ;
- Le Titre III pose le cadre de la lutte contre la cybercriminalité ;
- Le Titre IV est réservé aux dispositions finales.

Telle est l'objet du présent projet de loi que nous avons l'honneur de soumettre à votre approbation.

BURKINA FASO IV REPUBLIQUE

UNITE- PROGRES - JUSTICE SEPTIEME LEGISLATURE

ASSEMBLEE NATIONALE

AVANT-PROJET DE LOI N°...-2016/AN DU ……..2017 PORTANT PROMOTION DE LA CYBERSECURITE ET LUTTE CONTRE LA CYBERCRIMINALITE

L'ASSEMBLEE NATIONALE

VU la Constitution ;

VU la résolution N° 001-2015/AN du 30 décembre 2015 portant validation du mandat des députés ;

a délibéré en sa séance du……..
et adopté la loi dont la teneur suit :

TITRE PREMIER : DISPOSITIONS GENERALES

Article premier : Objet et champ d'application

La présente loi régit le cadre de cybersécurité au Burkina Faso. Elle met en place un dispositif permettant de prévenir et de faire face aux menaces et risques numériques, tout en garantissant la promotion et le développement des technologies de l'information et de la communication ainsi que de l'Economie numérique.

La présente loi vise également à assurer une protection pénale du système de valeurs de la société burkinabè de l'information en mettant en place les mécanismes juridiques et institutionnels appropriés à la lutte contre la cybercriminalité. Elle définit et réprime ainsi les infractions liées à l'utilisation des technologies de l'information et de la communication au Burkina Faso.

Article 2 : Définitions

Au sens de la présente loi et de ses textes d'application, les différentes expressions suivantes sont définies comme suit :

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

2) **Algorithme** : suite d'opérations mathématiques élémentaires à appliquer à des données pour aboutir à un résultat désiré ;

3) **Algorithme symétrique** : algorithme de déchiffrement utilisant une même clé pour chiffrer et déchiffrer les messages ;

4) **Algorithme asymétrique** : algorithme de chiffrement utilisant une clé publique pour chiffrer et une clé privée (différente) pour déchiffrer les messages ;

5) **Attaque active** : acte modifiant ou altérant les ressources ciblées par l'attaque (atteinte à l'intégrité, à la disponibilité et à la confidentialité des données) ;

6) **Attaque passive** : acte n'altérant pas sa cible (écoute passive, atteinte à la confidentialité) ;

7) **Atteinte à l'intégrité** : fait de provoquer intentionnellement une perturbation grave ou une interruption de fonctionnement d'un système d'information, d'un réseau de communications électroniques ou d'un équipement terminal, en introduisant, transmettant, endommageant, effaçant, détériorant, modifiant, supprimant ou rendant inaccessibles des données ;

8) **Audit de sécurité** : examen méthodique des composantes et des acteurs de la sécurité, de la politique, des mesures, des solutions, des procédures et des moyens mis en œuvre par une organisation, pour sécuriser son environnement, effectuer des contrôles de conformité, des contrôles d'évaluation de l'adéquation des moyens (organisationnels, techniques, humains, financiers) investis au regard des risques encourus, d'optimisation, de rationalité et de performance ;

9) **Authentification** : critère de sécurité défini par un processus mis en œuvre notamment pour vérifier l'identité d'une personne physique ou morale et s'assurer que l'identité correspond à l'identité de cette personne préalablement enregistrée ;

10) **Chiffrement** : toute technique qui consiste à transformer des données numériques en un format inintelligible en employant des moyens de cryptologie ;

11) **Clé** : dans un système de chiffrement, elle correspond à une valeur mathématique, un mot, une phrase qui permet, grâce à l'algorithme de chiffrement, de chiffrer ou de déchiffrer un message ;

12) **Clé privée** : clé utilisée dans les mécanismes de chiffrement asymétrique (ou chiffrement à clé publique), qui appartient à une entité et qui doit être secrète ;

13) **Clé publique** : clé servant au chiffrement d'un message dans un système asymétrique et donc librement diffusé ;

14) **Clé sécrète** : clé connue de l'émetteur et du destinataire servant de chiffrement et de déchiffrement des messages et utilisant le mécanisme de chiffrement symétrique ;

15) **Code source** : ensemble des spécifications techniques, sans restriction d'accès ni de mise en œuvre, d'un logiciel ou protocole de communication, d'interconnexion, d'échange ou d'un format de données ;

16) **Code de conduite** : ensemble des règles élaborées par le responsable du traitement afin d'instaurer un usage correct des ressources informatiques, des réseaux et des communications électroniques de la structure concernée et homologué par l'Autorité de protection ;

17) **Commerce électronique** : l'acte d'offrir, d'acheter, ou de fournir des biens et des services via les systèmes informatiques et les réseaux de télécommunications comme le réseau Internet ou tout autre réseau utilisant des moyens électroniques, optiques ou d'autres supports analogues permettant des échanges d'informations à distance ;

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

19) **Communication électronique** : toute transmission 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 ;

20) **Confidentialité** : maintien du secret des informations et des transactions afin de prévenir la divulgation non autorisée d'informations aux non destinataires permettant la lecture, l'écoute, la copie illicite d'origine intentionnelle ou accidentelle durant leur stockage, traitement ou transfert ;

21) **Contenu** : ensemble d'informations relatives aux données appartenant à des personnes physiques ou morales, transmises ou reçues à travers les réseaux de communications électroniques et les systèmes d'information ;

22) **Contenu illicite** : contenu portant atteinte à la dignité humaine, à la vie privée, à l'honneur ou à la sécurité nationale ;

23) **Conventions secrètes** : les clés non publiées nécessaires à la mise en œuvre d'un moyen ou d'une prestation de cryptologie pour les opérations de chiffrement ou de déchiffrement ;

24) **Communication électronique indirecte** : tout message de texte, de voix, de son, d'image envoyé via un réseau de communication électronique et stocké sur le réseau ou sur un terminal de communication jusqu'à réception dudit message ;

25) **Consentement de la personne concernée** : toute manifestation de volonté expresse, non équivoque, libre, spécifique et informée par laquelle la personne concernée ou son représentant légal, judiciaire ou conventionnel accepte que ses données à caractère personnel fassent l'objet d'un traitement manuel ou électronique ;

26) **Courrier électronique** : tout message, sous forme de texte, de voix, de son ou d'image, envoyé par un réseau public de communication, stocké sur un serveur du réseau ou dans l'équipement terminal du destinataire, jusqu'à ce que ce dernier le récupère ;

27) **Cryptage** : utilisation de codes ou signaux non usuels permettant la conservation des informations à transmettre en des signaux incompréhensibles par les tiers ;

28) **Cryptanalyse** : ensemble des moyens qui permet d'analyser une information préalablement chiffrée en vue de la déchiffrer ;

29) **Cryptogramme** : message chiffré ou codé ;

30) **Cryptographie** : application des mathématiques permettant d'écrire l'information, de manière à la rendre inintelligible à ceux ne possédant pas les capacités de la déchiffrer ;

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

32) **Cryptologie (Moyens de)**: l'ensemble des outils scientifiques et techniques (matériel ou logiciel) qui permettent de chiffrer et/ou de déchiffrer ;

33) **Cryptologie (Prestation de)**: toute opération visant la mise en œuvre, pour le compte de soi ou d'autrui, des moyens de cryptologie ;

34) **Cryptologie (Activité de)**: toute activité ayant pour but la production, l'utilisation, l'importation, l'exportation ou la commercialisation des moyens de cryptologie ;

35) **Cybercriminalité** : ensemble des infractions s'effectuant à travers le cyberspace par des moyens autres que ceux habituellement mis en œuvre, et de manière complémentaire à la criminalité classique ;

36) **Cybersécurité** : 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 ;

37) **Déchiffrement** : opération inverse du chiffrement ;

38) **Déni de service** : attaque par saturation d'une ressource du système d'information ou du réseau de communications électroniques, afin qu'il s'effondre et ne puisse plus réaliser les services attendus de lui ;

39) **Déni de service distribué** : attaque simultanée des ressources du système d'information ou du réseau de communications électroniques, afin de les saturer et amplifier les effets d'entrave ;

40) **Dépasser un accès autorisé** : le fait d'accéder à un système d'information et d'utiliser un tel accès pour obtenir ou modifier des données dans une partie de l'ordinateur ou le titulaire n'est pas autorisé d'y accéder ;

41) **Disponibilité** : critère de sécurité permettant que les ressources des réseaux de communications électroniques, des systèmes d'information ou des équipements terminaux soient accessibles et utilisables selon les besoins (le facteur temps) ;

42) **Dispositif de création de signature électronique** : ensemble d'éléments logiciels ou matériels permettant la création d'une signature électronique ;

43) **Dispositif de vérification de signature électronique** : ensemble d'éléments logiciels ou matériels permettant la vérification d'une signature électronique ;

44) **Dommage** : toute atteinte à l'intégrité ou à la disponibilité des données, d'un programme, d'un système ou d'une information ;

45) **Données** : représentation de faits, d'informations ou de notions sous une forme susceptible d'être traitée par un équipement terminal, y compris un programme permettant à ce dernier d'exécuter une fonction ;

46) **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 ;

47) **Données de connexion** : ensemble de données relatives au processus d'accès dans une communication électronique ;

48) **Données de trafic** : données ayant trait à une communication électronique indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type du service sous-jacent ;

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

50) **Données sensibles** : toutes les données à caractère personnel relatives aux opinions ou activités religieuse, philosophique, politique, syndicale, à la vie sexuelle ou raciale, à la santé, aux mesures d'ordre social, aux poursuites, aux sanctions pénales ou administratives ;

51) **Double criminalité** : une infraction punie à la fois dans l'État où un suspect est détenu et un État demandant que le suspect soit remis ou transféré ;

52) **Equipement terminal** : appareil, installation ou ensemble d'installations destiné à être connecté à un point de terminaison d'un système d'information et émettant, recevant, traitant, ou stockant des données d'information ;

53) **Fournisseur des services de communications électroniques** : personne physique ou morale fournissant les prestations consistant entièrement ou principalement en la fourniture de communications électroniques ;

54) **Gravité de l'impact** : appréciation du niveau de gravité d'un incident, pondéré par sa fréquence d'apparition ;

55) **Information** : tout élément de connaissance susceptible d'être représenté à l'aide de conventions pour être utilisé, conservé, traité ou communiqué. L'information peut être exprimée sous forme écrite, visuelle, sonore, numérique, ou autre ;

56) **Infrastructure essentielle de l'information ou infrastructure critique de TIC/Cyberespace** : Infrastructure qui est essentielle aux services vitaux pour la sureté publique, la stabilité économique, la sécurité nationale, la stabilité internationale et pour la pérennité et la restauration du cyberespace critique ;

57) **Intégrité des données** : critère de sécurité définissant l'état d'un réseau de communications électroniques, d'un système d'information ou d'un équipement terminal qui est demeuré intact et permet de s'assurer que les ressources n'ont pas été altérées (modifiées ou détruites) d'une façon tant intentionnelle qu'accidentelle, de manière à assurer leur exactitude, leur fiabilité et leur pérennité ;

58) **Interception illégale** : 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 ;

59) **Interception légale** : accès autorisé aux données d'un réseau de communications électroniques, d'un système d'information ou d'un équipement terminal ;

60) **Interconnexion des données à caractère personnel** : tout mécanisme de connexion consistant en la mise en relation de données traitées pour une finalité déterminée avec d'autres données traitées pour des finalités identiques ou non, ou liées par un ou plusieurs responsables de traitement ;

61) **Intrusion par intérêt** : accès intentionnel et sans droit dans un réseau de communications électroniques ou dans un système d'information, dans le but soit de nuire soit de tirer un bénéfice économique, financier, industriel, sécuritaire ou de souveraineté ;

62) **Intrusion par défi intellectuel** : accès intentionnel et sans droit dans un réseau de communications électroniques ou dans un système d'information, dans le but de relever un défi intellectuel pouvant contribuer à l'amélioration des performances du système de sécurité de l'organisation ;

63) **Logiciel espion** : type particulier de logiciel trompeur collectant les informations personnelles (sites web les plus visités, mots de passe, etc.) auprès d'un utilisateur du réseau de communications électroniques ;

64) **Logiciel potentiellement indésirable** : logiciel représentant des caractéristiques d'un logiciel trompeur ou d'un logiciel espion ;

65) **Logiciel trompeur** : logiciel effectuant des opérations sur un équipement terminal d'un utilisateur sans informer préalablement cet utilisateur de la nature exacte des opérations que ce logiciel va effectuer sur son équipement terminal ou sans demander à l'utilisateur s'il consent à ce que le logiciel procède à ces opérations ;

66) **Message clair** : version intelligible d'un message et compréhensible par tous ;

67) **Mineur ou Enfant** : toute personne physique âgée de moins de 18 ans au sens de la Charte Africaine sur les droits et le bien-être de l'Enfant et de la convention des Nations Unies sur les droits de l'enfant ;

68) **Moyen de cryptographie** : équipement ou logiciel conçu ou modifié pour transformer des données, qu'il s'agisse d'informations ou de signaux, à l'aide de conventions secrètes ou pour réaliser une opération inverse avec ou sans convention secrète afin de garantir la sécurité du stockage ou de la transmission de données, et d'assurer leur confidentialité et le contrôle de leur intégrité ;

69) **Moyen de paiement électronique** : moyen permettant à son titulaire d'effectuer des opérations de paiement électroniques en ligne ;

70) **Non répudiation** : critère de sécurité assurant la disponibilité de preuves qui peuvent être opposées à un tiers et utilisées pour prouver la traçabilité d'une communication électronique qui a eu lieu ;

71) **Politique de sécurité** : référentiel de sécurité établi par une organisation, reflétant sa stratégie de sécurité et spécifiant les moyens de la réaliser ;

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

73) **Prestataire de services de cryptologie** : toute personne, physique ou morale, qui fournit une prestation de cryptologie ;

74) **Personne concernée** : toute personne physique qui fait l'objet d'un traitement des données à caractère personnel ;

75) **Prospection directe** : tout envoi de message destiné à promouvoir, directement ou indirectement, des biens, des services ou l'image d'une personne vendant des biens ou fournissant des services ; elle vise aussi toute sollicitation effectuée au moyen de l'envoi de message, quel qu'en soit le support ou la nature notamment commerciale, politique ou caritative, destinée à promouvoir, directement ou indirectement, des biens, des services ou l'image d'une personne vendant des biens ou fournissant des services ;

76) **Raciste et xénophobe en matière des technologies de l'information et de la communication** : tout matériel écrit, toute image ou toute autre représentation d'idées ou de théories qui préconise ou encourage la haine, la discrimination ou la violence contre une personne ou un groupe de personnes, en raison de la race, de la couleur, de l'ascendance ou de l'origine nationale ou ethnique ou de la religion ;

77) **Sécurité** : situation dans laquelle quelqu'un, quelque chose n'est exposé à aucun danger. Mécanisme destiné à prévenir un événement dommageable, ou à limiter les effets ;

78) **Signature électronique** : une donnée sous forme électronique, qui est jointe ou liée logiquement à d'autres données électroniques et qui sert de procédé d'identification ;

79) **Sous-traitant** : toute personne physique ou morale, publique ou privée, tout autre organisme ou association qui traite des données pour le compte du responsable du traitement ;

80) **Système de détection** : système permettant de détecter les incidents qui pourraient conduire aux violations de la politique de sécurité et permettant de diagnostiquer des intrusions potentielles ;

81) **Système d'information** : 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 ;

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

83) **Vulnérabilité** : défaut de sécurité se traduisant soit intentionnellement, soit accidentellement par une violation de la politique de sécurité, dans l'architecture d'un réseau de Communications électroniques, dans la conception d'un système d'information.

Les termes et expressions non définis dans la présente loi, conservent leurs définitions ou significations données par les instruments juridiques internationaux auxquels le Burkina Faso a souscrit.

TITRE II : PROMOTION DE LA CYBERSECURITE

Chapitre premier : Cadre politique et stratégique de la cybersécurité

Article 3 : Politique nationale de cybersécurité

Le Gouvernement du Burkina Faso, en collaboration avec toutes les parties prenantes et par le biais du ministère en charge de la Sécurité nationale, définit la politique nationale de cybersécurité.

La politique nationale de cybersécurité identifie et reconnait l'importance des infrastructures essentielles de l'information pour la nation. Elle identifie en outre les risques auxquels les

infrastructures essentielles de l'information sont confrontées. Enfin, la politique nationale de cyber sécurité définit, dans les grandes lignes, les objectifs de l'Etat en matière de cybersécurité ainsi que les modalités selon lesquelles de tels objectifs sont mis en œuvre.

Article 4 : Stratégies nationales de cybersécurité

Pour assurer la mise en œuvre de la politique nationale de cybersécurité, le ministère en charge de la Sécurité nationale, en collaboration avec le ministère en charge de l'Economie numérique, définie et met en œuvre les stratégies appropriées et suffisantes, en tenant compte de l'évolution technologique et des priorités du gouvernement dans ce domaine. A cette fin, le ministère en charge de la Sécurité nationale est assisté par la structure nationale spécialisée en matière de cybersécurité.

Les stratégies nationales de cybersécurité peuvent notamment être constituées autour des axes suivants :

1) les réformes du dispositif juridique et institutionnel indispensables à l'amélioration et au développement du cadre de la cybersécurité ;
2) la promotion d'un leadership nationale pour le développement de la culture de la sécurité ;
1) la promotion d'une culture de la cybersécurité chez toutes les parties prenantes ;
2) la sensibilisation et le développement des capacités des acteurs clés ;
3) les mécanismes de renforcement de la souveraineté numérique ;
4) le partenariat public-privé et la coopération internationale.

Les stratégies nationales de cybersécurité établissent des structures organisationnelles et se fixent des objectifs ainsi que des délais pour mener à bien tous les aspects de la politique de cybersécurité, tout en posant les bases d'une gestion effective des volets prévention, protection, détection et riposte relatifs aux incidents de cybersécurité.

Chapitre II : Cadre de gouvernance de la cybersécurité

Article 5 : Autorité gouvernementales de gouvernance de la cybersécurité

Le ministère en charge de la Sécurité nationale est l'autorité gouvernementale en matière de cybersécurité. Il assure, sous l'autorité du Premier ministre et en collaboration avec le ministère en charge de l'Economie numérique, la gouvernance stratégique de la cybersécurité au Burkina Faso.

Article 6 : Agence nationale de la cybersécurité

Il est créé une autorité administrative indépendante à compétence nationale dénommé " Agence Nationale de la Cybersécurité ", en abrégé « ANC ». L'Agence Nationale de la Cybersécurité est rattaché au ministère en charge de la Sécurité nationale.

L'Agence Nationale de la Cybersécurité est l'autorité nationale en matière de sécurité des systèmes d'information. Il concourt de manière significative à la définition et à la mise en œuvre de la politique et des orientations stratégiques en matière de cybersécurité.

A ce titre, l'Agence Nationale de la Cybersécurité :

1) assure la fonction d'autorité nationale de défense des systèmes d'information. En cette qualité, elle :
    a) propose aux autorités gouvernementales compétentes les mesures destinées à répondre aux crises affectant ou menaçant la sécurité des infrastructures essentielles de l'information, des systèmes d'information des autorités publiques et des opérateurs d'importance vitale ;
    b) coordonne, dans le cadre des orientations fixées par les autorités gouvernementales compétentes, l'action gouvernementale en matière de défense des systèmes d'information ;

2) conçoit, fait réaliser et met en œuvre les moyens interministériels sécurisés de communications électroniques nécessaires au Président de la République et au Gouvernement ;

3) anime et coordonne les travaux interministériels en matière de sécurité des systèmes d'information ;

4) élabore les mesures de protection des systèmes d'information proposées au ministère en charge de la Sécurité et de la protection civile ou au Premier ministre et veille à l'application des mesures adoptées ;

5) identifie les infrastructures essentielles de l'information considérées comme les secteurs considérés comme sensibles pour sa sécurité nationale et le bien-être de l'économie et des systèmes technologies de l'information et de la communication ;

6) mène des inspections et audits des systèmes d'information des services de l'Etat des infrastructures essentielles de l'information et des opérateurs d'importance vitale ;

7) met en œuvre un système de détection et d'évaluation des menaces ou des évènements susceptibles d'affecter la sécurité des systèmes d'information de l'Etat et coordonne la réaction à ces évènements ;

8) recueille les informations techniques relatives aux incidents affectant les infrastructures essentielles de l'information, les systèmes d'information de l'Etat et des opérateurs d'importance vitale ;

9) délivre des agréments aux dispositifs et aux mécanismes de sécurité destinés à protéger, dans les systèmes d'information, les informations couvertes par le secret de la défense nationale ;

10) participe aux négociations internationales et assure la liaison avec ses homologues étrangers ;

11) assure la sensibilisation et la formation des personnels qualifiés dans le domaine de la sécurité des systèmes d'information.

Les attributs et missions ainsi que les modalités d'organisation et de fonctionnement de l'Agence Nationale de la Cybersécurité sont précisés par décret.

TITRE III : LUTTE CONTRE LA CYBERCRIMINALITE

Chapitre premier : Infractions et peines en matière de cybercriminalité

Section première : atteintes aux systèmes informatiques

Article 7 : Accès frauduleux à un système informatique

Quiconque accédé ou tente d'accéder frauduleusement à tout ou partie d'un système informatique, est puni d'un (1) à trois (3) ans d'emprisonnement et d'une amende de 1.000.000 à 10.000.000 francs CFA 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 8 : Maintien frauduleux à un système informatique

Quiconque se maintient ou tente de se maintenir frauduleusement dans tout ou partie d'un système informatique, est puni d'un (1) à trois (3) ans d'emprisonnement et d'une amende de 1.000.000 à 10.000.000 francs CFA ou de l'une de ces deux peines seulement.

Article 9 : Entrave au fonctionnement d'un système informatique

Quiconque entrave ou fausse ou tente d'entraver ou de fausser le fonctionnement d'un système informatique, est puni d'un (1) à cinq (5) ans d'emprisonnement et d'une amende de 1.000.000 à 10.000.000 francs CFA ou de l'une de ces deux peines seulement.

Article 10 : Introduction frauduleuse de données dans un système informatique

Quiconque accède ou tente d'accéder frauduleusement, introduit ou tente d'introduire frauduleusement des données dans un système informatique, est puni d'un (1) à cinq (5) ans d'emprisonnement et d'une amende de 1.000.000 à 10.000.000 francs CFA ou de l'une de ces deux peines seulement.

Section II : Atteintes aux données informatisées

Article 11 : Interception frauduleuse de données informatiques

Quiconque intercepte ou tente 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, est puni d'un (1) à cinq (5) ans d'emprisonnement et d'une amende de 1.000.000 à 10.000.000 francs CFA ou de l'une de ces deux peines seulement.

Article 12 : Modification frauduleuse de données informatiques

Quiconque endommage ou tente d'endommager, efface ou tente d'effacer, détériore ou tente de détériorer, altère ou tente d'altérer, modifie ou tente de modifier, frauduleusement des données informatisées, est puni d'un (1) à cinq (5) ans d'emprisonnement et d'une amende de 1.000.000 à 10.000.000 francs CFA ou de l'une de ces deux peines seulement.

Article 13 : Modification frauduleuse de données informatiques

Quiconque endommage ou tente d'endommager, efface ou tente d'effacer, détériore ou tente de détériorer, altère ou tente d'altérer, modifie ou tente de modifier, frauduleusement des données informatisées, est puni d'un (1) à cinq (5) ans d'emprisonnement et d'une amende de 1.000.000 à 10.000.000 francs CFA ou de l'une de ces deux peines seulement.

Article 14 : Falsification de données informatiques

Quiconque produit ou fabrique 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, est puni d'un (1) à cinq (5) ans d'emprisonnement et d'une amende de 1.000.000 à 10.000.000 francs CFA ou de l'une de ces deux peines seulement.

Est puni des mêmes peines celui qui, en connaissance de cause, fait usage ou tente de faire usage des données obtenues dans les conditions prévues à l'alinéa premier du présent article.

Article 15 : Fraude informatique

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, est puni d'un (1) à cinq (5) ans d'emprisonnement et d'une amende de 1.000.000 à 10.000.000 francs CFA ou de l'une de ces deux peines seulement.

Section III : Infractions se rapportant au contenu

Article 16 : Production d'une image ou d'une représentation à caractère pornographique infantile

Quiconque produit, enregistre, offre, met à disposition, diffuse, transmet une image ou une représentation présentant un caractère de pornographie infantile par le biais d'un système informatique, est puni de cinq (5) à dix (10) ans d'emprisonnement et d'une amende de 1.000.000 à 15.000.000 francs CFA ou de l'une de ces deux peines seulement.

Article 17 : Importation ou exportation d'une image ou d'une représentation à caractère pornographique infantile

Quiconque se procure ou procure à autrui, importe ou fait importer, exporte ou fait exporter une image ou une représentation présentant un caractère de pornographie infantile par le biais d'un système informatique, est puni de cinq (5) à dix (10) ans d'emprisonnement et d'une amende de 1.000.000 à 15.000.000 francs CFA ou de l'une de ces deux peines seulement.

Article 18 : Possession d'une image ou d'une représentation à caractère pornographique infantile

Quiconque 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, est puni de cinq (5) à dix (10) ans d'emprisonnement et d'une amende de 1.000.000 à 15.000.000 francs CFA ou de l'une de ces deux peines seulement.

Article 19 : Possession d'une image ou d'une représentation à caractère pornographique infantile

Quiconque facilite l'accès à des images, des documents, du son ou une représentation présentant un caractère de pornographie à un mineur, est puni de cinq (5) à dix (10) ans d'emprisonnement et d'une amende de 1.000.000 à 15.000.000 francs CFA ou de l'une de ces deux peines seulement.

Article 20 : Facilitation d'accès à des images, des documents, du son ou une représentation présentant un caractère de pornographie à un mineur

Quiconque facilite l'accès à des images, des documents, du son ou une représentation présentant un caractère de pornographie à un mineur, est puni de cinq (5) à dix (10) ans d'emprisonnement et d'une amende de 1.000.000 à 15.000.000 francs CFA ou de l'une de ces deux peines seulement.

Article 21 : Disposition d'écrits ou d'images de nature raciste ou xénophobe par le biais d'un système informatique

Quiconque crée, télécharge, diffuse ou met 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, est puni d'un (1) à cinq (5) ans d'emprisonnement et d'une amende de 1.000.000 à 15.000.000 francs CFA ou de l'une de ces deux peines seulement.

Article 22 : Menace par le biais d'un système informatique

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, est puni d'un (1) à cinq (5) ans d'emprisonnement et d'une amende de 1.000.000 à 15.000.000 francs CFA ou de l'une de ces deux peines seulement.

Article 23 : Injure commise par le biais d'un système informatique

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, est puni d'un (1) à cinq (5) ans d'emprisonnement et d'une amende de 1.000.000 à 15.000.000 francs CFA ou de l'une de ces deux peines seulement.

Article 24 : Négationnisme

Quiconque nie, approuve ou justifie intentionnellement des actes constitutifs de génocide ou de crimes contre l'humanité par le biais d'un système informatique, est puni d'un (1) à cinq (5) ans d'emprisonnement et d'une amende de 1.000.000 à 15.000.000 francs CFA ou de l'une de ces deux peines seulement.

Section IV : Infractions liées aux activités des prestataires techniques de services de communication au public par voie électronique.

Article 25 : Présentation d'un contenu ou d'une activité comme illicite

Quiconque présente aux personnes mentionnées l'alinéa 2 de l'article 10 de la loi sur les transactions électroniques, un contenu ou une activité comme étant illicite dans le but d'en obtenir le retrait ou d'en faire cesser la diffusion, alors qu'elle sait cette information inexacte, est puni d'un emprisonnement de six (6) mois à un (1) an et d'une amende de 200.000 à 1.000.000 francs CFA ou de l'une de ces deux peines seulement.

Article 26 : Non respect des obligations des prestataires de services

Toute personne physique ou tout dirigeant de droit ou de fait d'une personne morale exerçant l'une des activités définies aux alinéas 1 et 2 de l'article 10 de la loi sur les transactions électroniques, qui ne satisfait pas aux obligations définies à l'article 13 de la loi sur les transactions électroniques, ne conserve pas les éléments d'information visés à l'article 15 de la loi susvisée ou n'a pas déféré à la demande d'une autorité judiciaire d'obtenir communication desdits éléments est puni d'un emprisonnement de six (6) mois à un (1) an et d'une amende de 100.000 à 500.000 francs CFA ou de l'une de ces deux peines seulement.

Article 27 : Défaut de mention des moyens techniques existants

Toute personne physique ou tout dirigeant de droit ou de fait d'une personne morale exerçant l'activité définie à l'article 10 de la loi sur les transactions électroniques, n'ayant pas respectée les prescriptions de ce même article est puni d'un emprisonnement de six (6) mois à un (1) an et d'une amende de 200.000 à 1.000.000 francs CFA ou de l'une de ces deux peines seulement.

Article 28 : Non respect des prescription en matière de lutte contre les contenus illicite

Toute personne physique ou tout dirigeant de droit ou de fait d'une personne morale exerçant l'activité définie à l'article 10 de la loi sur les transactions électroniques, n'ayant pas respectée les prescriptions prévues à l'article 23 de la même loi est puni d'un an d'emprisonnement de six (6) mois à un (1) an et d'une amende de 200.000 à 2.000.000 francs CFA ou de l'une de ces deux peines seulement.

Article 29 : Non respect des prescriptions relatives l'exercice du droit de réponse

Tout directeur de publication est tenu de publier la réponse portant sur l'exercice du droit de réponse, en application de l'article 25 de la loi sur les transactions électroniques, vingt quatre (24) heures, après la réception de la demande sous peine d'une amende de 200.000 à 20.000.000 francs CFA, sans préjudice de toutes autres peines prévues par la législation en vigueur.

Article 30 : Manquement à l'obligation d'information du consommateur

Les dispositions de l'article 26 de la présente loi s'appliquent pour tout manquement à l'obligation d'information du consommateur prévue aux articles 31 et suivants de la loi sur les transactions électroniques.

Article 31 : Refus de remboursement consécutif à l'exercice du droit de rétractation

Le refus d'un fournisseur électronique de biens ou de services de rembourser les montants reçus d'un consommateur qui exerce son droit de rétraction est passible d'un

d'emprisonnement de six (6) mois à un (1) an et d'une amende de 200.000 à 2.000.000 francs CFA ou de l'une de ces deux peines seulement.

Article 32 : Livraison frauduleuse d'un bien

Est puni d'un emprisonnement d'un (1) mois à un (1) an et d'une amende de 500.000 à 10.000.000 francs CFA, ou l'une de ces peines seulement, celui qui trompe l'acheteur sur l'identité, la nature ou l'origine du bien vendu, en livrant frauduleusement un bien autre que celui commandé et acheté par le consommateur.

Section V : Infractions liées à la publicité par voie électronique

Article 33 : Méconnaissance des conditions d'accès aux offres promotionnelles

Quiconque méconnait les conditions auxquelles sont soumises la possibilité de bénéficier d'offres promotionnelles ainsi que celles de participer à des concours ou à des jeux promotionnels, lorsque ces offres, concours ou jeux sont proposés par voie numérique, telles que prévues à l'article 36 de la loi sur les transactions électroniques est puni d'un emprisonnement de six (6) mois à deux (2) ans et d'une amende de 100.000 à 500.000 francs CFA ou de l'une de ces deux peines seulement.

Article 34 : Méconnaissance des conditions d'identification des offres promotionnelles

Quiconque réalise des publicités, et notamment les offres promotionnelles, telles que les rabais, les primes ou les cadeaux, ainsi que les concours ou les jeux promotionnels, adressés par courrier électronique, en violation de l'article 36 de la loi sur les transactions électroniques est puni d'un emprisonnement de six (6) mois à deux (2) ans et d'une amende de 100.000 à 500.000 francs CFA ou de l'une de ces deux peines seulement.

Section VII : atteintes spécifiques aux droits de la personne au regard du traitement des données à caractère personnel.

Article 35 : Non respect les formalités préalables

Quiconque, même par négligence, procède ou fait procéder à des traitements de données à caractère personnel sans avoir respecté les formalités préalables à leur mise en œuvre prévues par la loi sur les données à caractère personnel, est puni d'un emprisonnement d'un (1) an à sept (7) ans et d'une amende de 500.000 francs à 10.000.000 francs ou de l'une de ces deux peines seulement.

Article 36 : Méconnaissance des mesures d'interruption

Quiconque, même par négligence, procède ou fait procéder à un traitement qui a fait l'objet de la mesure d'interruption de mise en œuvre du traitement, conformément à la loi sur les données à caractère personnel, est puni d'un emprisonnement d'un (1) an à sept (7) ans et

d'une amende de 500.000 francs à 10.000.000 francs ou de l'une de ces deux peines seulement.

Article 37 : Non respect des normes simplifiées

Lorsqu'il est procédé ou fait procéder à un traitement de données à caractère personnel dans les conditions prévues par l'article 39 de la loi sur les données à caractère personnel précitée, quiconque ne respecte pas, y compris par négligence, les normes simplifiées ou d'exonération établies à cet effet par la Commission de l'Informatique et des Libertés, est puni d'un d'emprisonnement d'un (1) an à sept (7) ans et d'une amende de 500.000 francs à 10.000.000 francs ou de l'une de ces deux peines seulement.

Article 38 : Traitement non autorisé incluant le numéro d'inscription des personnes au répertoire national d'identification

Quiconque, hors les cas où le traitement a été autorisé dans les conditions prévues par la loi sur les données à caractère personnel précitée, procède ou fait procéder à un traitement de données à caractère personnel incluant parmi les données sur lesquelles il porte le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques, est puni d'un emprisonnement d'un (1) an à sept (7) ans et d'une amende de 500.000 francs à 10.000.000 francs ou de l'une de ces deux peines seulement.

Article 39 : Non respect des mesures de sécurité et de conservation

Quiconque procède ou fait procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures de sécurité et de conservation prescrites à l'article 34 la loi sur les données à caractère personnel précitée, est puni d'un emprisonnement d'un (1) an à sept (7) ans et d'une amende de 500.000 francs à 10.000.000 francs ou de l'une de ces deux peines seulement.

Article 40 : Collecte frauduleuse, déloyale ou illicite de données à caractère personnel

Quiconque collecte des données à caractère personnel par un moyen frauduleux, déloyal ou illicite, est puni d'un emprisonnement d'un (1) an à sept (7) ans et d'une amende de 500.000 francs à 10.000.000 francs ou de l'une de ces deux peines seulement.

Article 41 : Non respect du doit d'opposition

Quiconque procède ou fait procéder à un traitement de données à caractère personnel concernant une personne physique malgré l'opposition de cette personne conformément à la loi sur les données à caractère personnel, lorsque ce traitement répond à des fins de prospection, notamment commerciale, ou lorsque cette opposition est fondée sur des motifs légitimes, est puni d'un emprisonnement d'un (1) an à sept (7) ans et d'une amende de 500.000 francs à 10.000.000 francs ou de l'une de ces deux peines seulement.

Article 42 : Traitement de données sensibles

Quiconque, hors les cas prévus par la loi, met ou conserve sur support ou mémoire informatique, sans le consentement exprès de l'intéressé, des données à caractère personnel qui, directement ou indirectement, font apparaître l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, ou les appartenances syndicales, ou qui sont relatives à la santé ou à l'orientation sexuelle de celui-ci, sera puni d'un emprisonnement d'un (1) an à sept (7) ans et d'une amende de 500.000 francs à 10.000.000 francs ou de l'une de ces deux peines seulement.

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

Article 43 : Traitement de données à caractère personnel relatives aux infractions, condamnations ou mesures de sûreté

Quiconque, hors les cas prévus par la loi, met ou conserve sur support ou mémoire informatique des données à caractère personnel concernant des infractions, des condamnations ou des mesures de sûreté, est puni des mêmes peines.

Article 44 : Traitement illicite de données ayant pour fin la recherche dans le domaine de la santé

En cas de traitement de données à caractère personnel ayant pour fin la recherche dans le domaine de la santé, est puni des mêmes peines, quiconque procède à un traitement :

1) sans avoir préalablement informé individuellement les personnes sur le compte desquelles des données à caractère personnel sont recueillies ou transmises de leur droit d'accès, de rectification et d'opposition, de la nature des données transmises et des destinataires de celles-ci ainsi que des dispositions prises pour leur traitement, leur conservation et leur protection ;

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

Article 45 : Violation des obligations de conservation

Quiconque conserve des données à caractère personnel au-delà de la durée nécessaire prévue par la loi sur les données à caractère personnel, sauf si cette conservation est effectuée à des fins historiques, statistiques ou scientifiques dans les conditions prévues par la loi, est puni d'un emprisonnement d'un (1) an à sept (7) ans et d'une amende de 500.000 francs à 10.000.000 francs ou de l'une de ces deux peines seulement.

Article 46 : Traitement illicite de données conservées au-delà de la durée nécessaire

Quiconque, hors les cas prévus par la loi, traite à des fins autres qu'historiques, statistiques ou scientifiques des données à caractère personnel conservées au-delà de la durée nécessaire prévue par la loi sur les données à caractère personnel est puni des mêmes peines.

Article 47 : Détournement de finalité

Quiconque, détenant des données à caractère personnel à l'occasion de leur enregistrement, de leur classement, de leur transmission ou de toute autre forme de traitement, détourne ces informations de leur finalité telle que définie par la disposition législative, l'acte réglementaire ou la décision de la Commission de l'Informatique et des Libertés autorisant le traitement automatisé, ou par les déclarations préalables à la mise en œuvre de ce traitement, est puni d'un emprisonnement d'un (1) an à sept (7) ans et d'une amende de 500.000 francs à 10.000.000 francs ou de l'une de ces deux peines seulement.

Article 48 : Atteinte à la considération ou à l'intimité de la personne concernée

Quiconque recueille, à l'occasion de leur enregistrement, de leur classement, de leur transmission ou d'une autre forme de traitement, des données à caractère personnel dont la divulgation a pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée, porte, sans autorisation de l'intéressé, ces données à la connaissance d'un tiers qui n'a pas qualité pour les recevoir, est puni d'un emprisonnement d'un (1) an à sept (7) ans et d'une amende de 500.000 francs à 10.000.000 francs ou de l'une de ces deux peines seulement.

Lorsque la divulgation prévue à l'alinéa précédent du présent article est commise par imprudence ou négligence, le responsable est puni d'un emprisonnement de six (6) mois à cinq (5) ans et d'une amende de 300.000 francs à 5.000.000 francs ou de l'une de ces deux peines seulement.

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

Article 49 : Entrave à l'action de la Commission de l'Informatique et des Libertés

Est puni d'emprisonnement de six (6) mois à deux (2) ans et d'une amende de 200.000 francs à 1.000.000 francs ou de l'une de ces deux peines seulement, quiconque entrave l'action de la Commission de l'Informatique et des Libertés :

1) soit en s'opposant à l'exercice des missions confiées à ses membres ou aux agents habilités en application de la loi sur les données à caractère personnel ;
2) soit en refusant de communiquer à ses membres ou aux agents habilités en application de la loi sur les données à caractère personnel, les renseignements et documents utiles à leur mission, ou en dissimulant lesdits documents ou renseignements, ou en les faisant disparaître ;

3) soit en communiquant des informations qui ne sont pas conformes au contenu des enregistrements tel qu'il était au moment où la demande a été formulée où qui ne présentent pas ce contenu sous une forme directement accessible

Section VI : Adaptation des infractions classiques aux technologies de l'information et de la communication

Article 50 : Vol d'information ou de données

La soustraction frauduleuse d'information ou de données au préjudice d'autrui est assimilée au vol.

Article 51 : circonstances aggravantes

Le fait d'utiliser les TIC ou d'agir en bande organisée en vue de commettre des infractions de droit commun comme le vol, l'escroquerie, le recel, l'abus de confiance, l'extorsion de fonds, le terrorisme, le blanchiment de capitaux constitue une circonstance aggravante de ces infractions au sens de la présente loi.

Lorsque les délits visés au premier alinéa du présent article ont été commis par le biais d'un système informatique, les peines prévues dans le code pénal ou autre texte législatif en vigueur pour les sanctionner peuvent être portées au double.

Lorsque les infractions ont été commises par le biais d'un système informatique, il ne peut être prononcé le sursis à l'exécution des peines.

Les infractions prévues dans la présente loi, lorsqu'elles ont été commises en bande organisée, sont punies des peines prévues respectivement pour l'infraction elle même ou pour l'infraction la plus sévèrement réprimée.

Article 52 : Infractions de droit commun commises sur les logiciels et programmes informatiques

Quiconque commet un vol, une escroquerie, un recel, un abus de confiance, une extorsion de fonds, ou une contrefaçon portant sur les données informatiques, les logiciels et les programmes, est puni d'un (1) à cinq (5) ans d'emprisonnement et d'une amende de 1.000.000 à 15.000.000 francs CFA ou de l'une de ces deux peines seulement.

Article 53 : Acte de terrorisme au moyen des TIC

Quiconque utilise ou tente d'utiliser les technologies de l'information et de la communication en vue de commettre un ou des actes de terrorisme, est puni de cinq (5) à dix (10) ans d'emprisonnement et d'une amende de 5.000.000 à 20.000.000 francs CFA ou de l'une de ces deux peines seulement.

Toute personne complice de la commission de l'infraction prévue au premier alinéa du présent article est punie des mêmes peines.

Article 54 : Acte de terrorisme visant les logiciels et programmes informatiques

Quiconque commet ou tente de commettre un ou des actes de terrorisme visant des logiciels et/ou programmes informatiques, est puni de cinq (5) à dix (10) ans d'emprisonnement et d'une amende de 5.000.000 à 20.000.000 francs CFA ou de l'une de ces deux peines seulement.

Toute personne complice de la commission de l'infraction prévue au premier alinéa du présent article est punie des mêmes peines.

Article 55 : Diffusion de procédés ou de moyens de destruction à des fins de terrorisme

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 un procédé, permettant la fabrication de moyens de destruction de nature à porter atteinte à la vie humaine, aux bien ou à l'environnement, est coupable d'acte de terrorisme et est puni de cinq (5) à dix (10) ans d'emprisonnement et d'une amende de 5.000.000 à 20.000.000 francs CFA ou de l'une de ces deux peines seulement.

Toute personne complice de la commission de l'infraction prévue au premier alinéa du présent article est punie des mêmes peines.

Article 56 : Incitation au suicide

Quiconque diffuse ou met à la disposition d'autrui par le biais d'un système informatique, un mode d'emploi, des information ou procédés d'incitation au suicide, est puni de cinq (5) à dix (10) ans d'emprisonnement et d'une amende de 5.000.000 à 20.000.000 francs CFA ou de l'une de ces deux peines seulement.

Toute personne complice de la commission de l'infraction prévue au premier alinéa du présent article est punie des mêmes peines.

Article 57 : Diffusion de fausses nouvelles tendant à faire croire à une situation d'urgence

Quiconque communique ou divulgue par le biais d'un système informatique, une fausse information tendant à faire croire qu'une destruction, une dégradation ou une détérioration de biens ou une atteinte aux personnes a été commise ou va être commise ou toute autre situation d'urgence, est puni de cinq (5) à dix (10) ans d'emprisonnement et d'une amende de 5.000.000 à 20.000.000 francs CFA ou de l'une de ces deux peines seulement.

Toute personne complice de la commission de l'infraction prévue au premier alinéa du présent article est punie des mêmes peines.

Article 58 : Menace de commettre un acte terroriste

Quiconque menace de commettre par le biais d'un système informatique, une destruction, une dégradation ou une détérioration de biens ou une atteinte aux personnes, lorsqu'une telle menace est matérialisée par un écrit, une image, une vidéo, un son ou toute autre données, est coupable de menace terroriste et est puni de six (6) mois à dix (5) ans d'emprisonnement et d'une amende de 1.000.000 à 10.000.000 francs CFA ou de l'une de ces deux peines seulement.

Toute personne complice de la commission de l'infraction prévue au premier alinéa du présent article est punie des mêmes peines.

Section VII : Infractions commises par tous moyens de diffusion publique

Article 59 : Atteinte au bonne mœurs par des moyens de diffusion publique

Quiconque :

1) fabrique ou détient en vue d'en faire commerce, distribution, location affichage ou exposition ;
2) importe ou fait importer, exporte ou fait exporter, transporte ou fait transporter sciemment aux mêmes fins ;
3) affiche, expose ou projette aux regards du public ;
4) vend, loue, met en vente ou en location, même non publiquement ;
5) offre, même à titre gratuit, même non publiquement sous quelque forme que ce soit, directement ou par moyen détourné ;
6) distribue ou remet en vue de leur distribution par un moyen quelconque,

tous imprimés, tous écrits, dessins, affiches, gravures, peintures, photographies, films ou clichés, matrices ou reproductions photographiques, emblèmes, tous objets ou images contraires aux bonnes mœurs, est puni de six (6) mois à dix (5) ans d'emprisonnement et d'une amende de 1.000.000 à 10.000.000 francs CFA ou de l'une de ces deux peines seulement.

Le maximum de la peine est prononcé lorsque les faits visés à l'alinéa premier du présent article ont un caractère pornographique.

Le condamné peut en outre faire l'objet, pour une durée ne dépassant pas six (6) mois, d'une interdiction d'exercer, directement ou par personne interposée, en droit ou en fait, des fonctions de direction de toute entreprise d'impression, d'édition ou de groupage et de distribution de journaux et de publications périodiques.

Quiconque contrevient à l'interdiction visée à l'alinéa 3 du présent article est puni des peines prévues au présent article.

Article 60 : Atteinte à la dignité humaine

Quiconque produit, diffuse ou met à la disposition d'autrui des données de nature à troubler l'ordre ou la sécurité publique ou de porter atteinte à la dignité humaine ou à l'intimité et à la vie privée d'une personne par le biais d'un système informatique, un mode d'emploi, des information ou procédés d'incitation au suicide, est puni d'un (1) à cinq (5) ans d'emprisonnement et d'une amende de 5.000.000 à 15.000.000 francs CFA ou de l'une de ces deux peines seulement.

Toute personne complice de la commission de l'infraction prévue au premier alinéa du présent article est punie des mêmes peines.

Section VIII : Atteintes à Sécurité publique et la défense nationale

Article 61 : Trahison

Est coupable de trahison et puni de la perpétuité tout burkinabè, qui :

1) livre à une puissance étrangère ou à ses agents, sous quelque forme ou par quelque moyen que se soit un renseignement, objet, document, procédé, donnée numérisée ou fichier informatisé qui doit être tenu secret dans l'intérêt de la défense nationale ;
2) s'assure, par quelque moyen que se soit, la possession d'un tel renseignement, objet, document, procédé, donnée informatisé ou fichier informatisé en vue de le livrer à une puissance étrangère ou à ses agents ;
3) détruit ou laisse détruire tel renseignement, objet, document, procédé, donnée numérisée ou fichier informatisé en vue de favoriser une puissance étrangère.

Article 62 : Atteinte au secret de défense nationale

Est puni du maximum des travaux forcés à temps, tout burkinabè ou tout étranger qui, dans l'intention de les livrer à tout pays tiers, rassemble des renseignements, objets, documents, procédés, données, logiciels, programme ou fichiers informatisés dont la réunion et l'exploitation sont de nature à nuire à la défense nationale.

Est puni de la détention criminelle de dix à vingt ans, tout gardien, tout dépositaire par fonction ou par qualité d'un renseignement, objet, document, procédé, donnée, logiciel, programme ou fichier informatisé qui doit être tenu secret dans l'intérêt de la défense nationale ou dont la connaissance pourrait conduire à la découverte d'un secret de défense nationale, qui sans 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.

La peine sera celle de la détention criminelle de cinq à dix ans si le gardien ou le dépositaire a agi par maladresse, imprudence, inattention, négligence ou inobservation des règlements.

Article 63 : Espionnage

Est coupable d'espionnage et puni de la perpétuité toute personne de nationalité étrangère, qui :

1) livre à une puissance étrangère ou à ses agents, sous quelque forme ou par quelque moyen que se soit un renseignement, objet, document, procédé, donnée numérisée ou fichier informatisé qui doit être tenu secret dans l'intérêt de la défense nationale ;
2) s'assure, par quelque moyen que se soit, la possession d'un tel renseignement, objet, document, procédé, donnée informatisé ou fichier informatisé en vue de le livrer à une puissance étrangère ou à ses agents ;
3) détruit ou laisse détruire tel renseignement, objet, document, procédé, donnée numérisée ou fichier informatisé en vue de favoriser une puissance étrangère.

Article 64 : Atteinte aux infrastructures essentielles de l'information

Lorsque les infractions définies aux articles 7 à 14 de la présente loi ont été commises en atteinte à un ou des systèmes informatiques protégés, considérés comme infrastructure critique de la défense nationale et/ou en raison des données critiques de sécurité nationale qu'ils contiennent, les peines prévues auxdits articles pour les sanctionner sont portées au double.

L'infraction d'atteinte à une infrastructure essentielles de l'information visée à l'alinéa premier du présent article inclut le fait de dépasser un accès autorisé.

Article 65 : Entrave à l'action des autorités nationales en charge de la cybersécurité

Est puni d'emprisonnement de six (6) mois à cinq (5) ans et d'une amende de 500.000 francs à 10.000.000 francs ou de l'une de ces deux peines seulement, quiconque entrave l'action des autorités nationales en charge de la cybersécurité ou de leur mandataire, y compris l'Agence Nationale de la Cybersécurité, soit :

1) en s'opposant à l'exercice des missions confiées à leurs membres ou agents habilités en application de la présente loi ou de ses textes d'application ;
2) en refusant de communiquer à leurs membres ou agents habilités en application de la présente loi ou de ses textes d'application, les renseignements et documents utiles à leur mission, ou en dissimulant lesdits documents ou renseignements, ou en les faisant disparaître ;
3) soit en communiquant des informations qui ne sont pas conformes au contenu des enregistrements tel qu'il était au moment où la demande a été formulée où qui ne présentent pas ce contenu sous une forme directement accessible.

Section IX : Autres infractions en matière de cybercriminalité

Article 66 : Disposition d'un équipement pour commettre des infractions

Quiconque produit, vend, importe, détient, diffuse, offre, cède ou met à disposition un équipement, un programme informatique, tout dispositif ou donnée conçue ou spécialement adaptée pour commettre une ou plusieurs des infractions prévues dans 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, est puni des peines prévues respectivement pour l'infraction elle même ou pour l'infraction la plus sévèrement réprimée.

Article 67 : Participation à une association formée ou à une entente en vue de commettre des infractions informatiques

Quiconque participe 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, est puni des peines prévues respectivement pour l'infraction elle même ou pour l'infraction la plus sévèrement réprimée.

Section X : Adaptation du régime de responsabilité pénale et de certaines sanctions à l'environnement numérique

Article 68 : Responsabilité des personnes morales

Les personnes morales, autres que l'Etat, les collectivités décentralisée 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 morales n'exclut pas celle des personnes physiques auteurs 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 ou, lorsqu'il s'agit d'un crime ou d'un délit puni en ce qui concerne les personnes physiques d'une peine d'emprisonnement supérieure à cinq (5) ans, détournée de son objet pour commettre les faits incriminés ;
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 de 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 69 : Confiscation des matériels ayant servi à commettre les infractions

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.

Article 70 : Interdictions à titre de peines complémentaires

En cas de 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, en couper l'accès par tous moyens techniques disponibles ou même en interdire l'hébergement.

Le juge peut faire injonction à toute personne responsable légalement du site ayant servi à commettre l'infraction, à toute personne qualifiée de mettre en œuvre les moyens techniques nécessaires en vue de garantir, l'interdiction d'accès, d'hébergement ou la coupure de l'accès au site incriminé.

La violation des interdictions prononcées par le juge est punie de six (6) à trois (3) ans d'emprisonnement et d'une amende de 5.000.000 à 5.000.000 francs CFA ou de l'une de ces deux peines seulement.

Article 71 : Publication de la décision de justice à titre de peines complémentaires

En cas de condamnation pour 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 premier du présent article doit être exécutée dans les quinze (15) jours suivant le jour où la condamnation est devenue définitive.

Le refus du condamné de faire diffuser ou de procéder à la diffusion de l'extrait dans les conditions définies au présent article est puni des peines prévues par le code pénal.

Si dans le délai de quinze (15) jours après que la condamnation soit devenue définitive, le condamné n'a pas diffusé ou fait diffuser cet extrait, les peines prévues au présent article sont portées au double.

Chapitre II : Règles de procédure pénale en matière de cybercriminalité

Article 72 : Prescription en matières d'infractions commises par le biais de réseaux numériques

Les crimes, délits et contraventions, lorsqu'ils sont commis par le biais de réseaux informatiques se prescriront dans les délais et suivant les distinctions établies par les articles 11 à 15 de la présente loi, à compter de la cessation de l'activité délictueuse en ligne.

Article 73 : Preuve électronique en matière pénale

L'écrit électronique en matière pénale est admis comme mode de preuve au même titre que l'écrit sur support papier à condition que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité.

Article 74 : Perquisition ou accès à un système informatique

Lorsque des données stockées dans un système informatique ou dans un support permettant de conserver des données informatisées sur le territoire du Burkina Faso, sont utiles à la manifestation de la vérité, l'Officier de police judiciaire 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 l'Officier de police judiciaire, sous réserve des conditions d'accès prévues par les engagements internationaux en vigueur.

Article 75 : Placement sous scellé de supports électroniques

Lorsque l'Officier de police judiciaire 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.

L'Officier de police judiciaire désigne toute personne qualifiée pour utiliser les moyens techniques appropriés afin d'empêcher l'accès aux données visées à l'article 49 de la présente loi dans le système informatique ou aux copies de ces données qui sont à la disposition de personnes autorisées à utiliser le système informatique et de garantir leur intégrité.

Si les données qui sont liées à l'infraction, soit qu'elles en constituent l'objet, soit qu'elles en ont été le produit, sont contraires à l'ordre public ou aux bonnes mœurs ou constituent un danger pour l'intégrité des systèmes informatiques ou pour des données stockées, traitées ou transmises par le biais de tels systèmes, l'Officier de police judiciaire ordonne les mesures conservatoires nécessaires, notamment en désignant toute personne qualifiée avec pour mission d'utiliser tous les moyens techniques appropriés pour rendre ces données inaccessibles.

Lorsque la mesure prévue à l'alinéa 2 du présent article n'est pas possible, pour des raisons techniques ou en raison du volume des données, l'Officier de police judiciaire utilise les moyens techniques appropriés pour empêcher l'accès à ces données dans le système informatique, de même qu'aux copies de ces données qui sont à la disposition de personnes autorisées à utiliser le système informatique, de même que pour garantir leur intégrité.

L'Officier de police judiciaire informe le responsable du système informatique de la recherche effectuée dans le système informatique et lui communique une copie des données qui ont été copiées, rendues inaccessibles ou retirées.

Article 76 : Placement sous scellé de supports électroniques

Si les nécessités de l'information l'exigent, l'Officier de police judiciaire peut utiliser les moyens techniques appropriés pour collecter ou enregistrer en temps réel, les données relatives au contenu de communications spécifiques, transmises au moyen d'un système informatique ou obliger un fournisseur de services, dans le cadre de ses capacités techniques à collecter ou à enregistrer, en application de moyens techniques existant, 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 77 : Pouvoirs des agents assermentés des structures nationales de cybersécurité et de lutte contre la cybercriminalité

Les agents assermentés des structures nationales de cybersécurité et de lutte contre la cybercriminalité, assistés au besoin par les forces de sécurité, peuvent, pour les nécessités de l'enquête ou de l'exécution d'une délégation judiciaire, procéder aux opérations prévues aux articles 74 à 76 de la présente loi.

TITRE IV : DISPOSITIONS FINALES

Article 78 : Dispositions finales

La présente loi abroge toute disposition antérieure contraire.

Des textes d'application fixent, en tant que de besoin, les modalités d'application de la présente loi.

La présente loi est exécutée comme loi de l'Etat.

Ainsi fait et délibéré en séance publique
à Ouagadougou, le ……

Le Secrétaire de séance

Le Président de l'Assemblée Nationale