BURKINA FASO

Unité-Progrès-Justice

IV^{E} REPUBLIQUE

TROISIEME LEGISLATURE DE TRANSITION

Session permanente

ASSEMBLEE LEGISLATIVE DE TRANSITION

COMMISSION DU DEVELOPPEMENT DURABLE (CDD)

RAPPORT N°2024-018/ALT/CDD

DOSSIER N°096 : **RELATIF AU PROJET DE LOI PORTANT SECURITE DES SYSTEMES D'INFORMATION AU BURKINA FASO**

Présenté au nom de la Commission du développement durable (CDD) par le député **Aboubacar KABRE**, rapporteur.

Juillet 2024

L'an deux mil vingt-quatre, le lundi 1er juillet, de 11 heures 00 minute à 20 heures 00 minute et le mardi 02 juillet, de 19 heures 10 minutes à 24 heures 00 minute, la Commission du développement durable (CDD) s'est réunie en séances de travail dans sa salle, sous la présidence du député Moussa KONE, Président de ladite Commission, à l'effet d'examiner le projet de loi portant sécurité des systèmes d'information au Burkina Faso.

Le Gouvernement était représenté par madame Aminata ZERBO/SABANE, Ministre de la Transition digitale, des postes et des communications électroniques. Elle était assistée de ses collaborateurs et des représentants du Ministère de la Justice et des droits humains, chargé des relations avec les institutions.

Les commissions générales, saisies pour avis, étaient représentées ainsi qu'il suit :

- la Commission des affaires étrangères, de la défense et de la sécurité (CAEDS) par la députée Sabine OUEDRAOGO/COMPAORE ;

- la Commission des finances et du budget (COMFIB) par le député Issaka TAPSOBA ;

- la Commission des affaires générales, institutionnelles et des droits humains (CAGIDH) par le député Jean Marie KOMBASSERE.

Le Président de la CDD, après avoir souhaité la bienvenue à la délégation gouvernementale, a proposé le plan de travail suivant qui a été adopté :

- audition du Gouvernement ;
- débat général ;
- examen du projet de loi article par article ;
- appréciation de la Commission.

En prélude à l'audition du Gouvernement et dans le souci de recueillir le maximum d'informations pour une législation consensuelle, la Commission a tenu une séance d'appropriation du projet de loi, le lundi 10 juin 2024 de 09 heures 00 minute à 13 heures 00 minute.

Elle a ensuite auditionné des acteurs qui exercent dans le domaine des systèmes d'information selon le chronogramme suivant :

Mardi 11 juin 2024

- de 14 heures 05 minutes à 15 heures 10 minutes : réunion zoom et en présentiel avec messieurs COULIBALY Idrissa, Ingénieur informaticien développeur et DAH Alfred, Spécialiste en sécurité informatique ;
- de 15 heures 15 minutes à 17 heures 10 minutes : la Fédération des associations du numérique (FED-numérique) et Internet Society Chapitre du Burkina Faso (ISOC-BF).

➢ **Mercredi 12 juin 2024**

- de 09 heures 05 minutes à 10 heures 05 minutes : le Conseil supérieur de la communication (CSC) ;
- de 10 heures 10 minutes à 12 heures 00 minute : la Commission de l'informatique et des libertés (CIL) ;
- de 12 heures 24 minutes à 13 heures 45 minutes : l'Autorité de régulation des communications électroniques et des postes (ARCEP) ;
- de 14 heures 25 minutes à 15 heures 40 minutes : la Brigade centrale de lutte contre la cybercriminalité (BCLCC) ;
- de 15 heures 45 minutes à 17 heures 15 minutes : l'Agence nationale de sécurité des systèmes d'information (ANSSI) ;
- de 17 heures 30 minutes à 18 heures 55 minutes : l'Agence nationale de promotion des technologies de l'information et de la communication (ANPTIC).

Certains acteurs invités n'ont pas pu honorer leur rendez-vous. D'autres par contre, outre leur participation, ont reversé des observations écrites et divers documents à la Commission qui l'ont éclairée lors de l'audition du Gouvernement.

I. AUDITION DU GOUVERNEMENT

Le Gouvernement a présenté l'exposé des motifs du projet de loi en trois points :

- contexte et justification ;
- processus d'élaboration du projet de loi ;
- contenu du projet de loi.

I.1. CONTEXTE ET JUSTIFICATION

Le développement fulgurant des Technologies de l'information et de la communication (TIC) a révolutionné les modes de travail des organisations et induit des changements profonds dans les modèles de société à travers le monde. Pour les Etats, ces technologies apportent de nouvelles perspectives pour l'amélioration de la gouvernance, la dynamisation de l'économie, la mise en œuvre des services sociaux de base et la création d'emplois. En effet, les TIC constituent un puissant levier de développement et sont désormais sollicitées à travers la mise en place de systèmes d'information de plus en plus critiques pour le fonctionnement de différentes organisations. Cependant, alors que les systèmes d'information apparaissent de plus en plus indispensables, ils sont exposés à des menaces de sécurité qui peuvent compromettre la survie des organisations. Dès lors, la sécurité des systèmes d'information devient un enjeu majeur.

Dans le monde matériel, les destructions causées par les guerres ou le terrorisme sont toujours visibles et beaucoup médiatisées. Cependant, dans le monde immatériel du cyberespace, les conséquences potentiellement néfastes des attaques informatiques contre les systèmes d'information des États, des entreprises ou contre les équipements des citoyens ordinaires, ne sont pas suffisamment vulgarisées pour le grand public.

Pourtant, l'imbrication entre le numérique et l'activité humaine est de plus en plus forte, faisant du cyberespace un lieu d'affrontement : vol de données personnelles, espionnage du patrimoine scientifique, économique et commercial d'entreprises par leurs concurrents ou par des puissances étrangères, arrêt de services nécessaires au bon fonctionnement de l'économie ou de la vie quotidienne, compromission d'informations de souveraineté, arnaque de tout genre et même, dans des circonstances de plus en plus récurrentes, perte de vies humaines.

Les risques liés à la sécurité des systèmes d'information sont accrus du fait que les systèmes informatiques sont de plus en plus connectés au réseau Internet et deviennent donc des ressources accessibles à distance, faisant ainsi d'eux des cibles potentielles d'attaques, notamment en termes d'intrusion, de déni de service ou simplement d'accès illicite. Au-delà des systèmes attaqués, ce sont les informations manipulées à travers ces réseaux qui sont convoitées.

L'Etat étant garant du développement de toutes les activités économiques, non seulement dans le monde matériel, mais également dans le cyberespace, doit mettre à la disposition des personnes :

- des infrastructures informationnelles fiables et sécurisées (accessibles, disponibles, fonctionnelles avec une garantie de la continuité des services) ;
- un cadre législatif et institutionnel adapté aux nouvelles menaces ;
- des instances judiciaire et policière compétentes dans le domaine des TIC et capables de coopérer au niveau international avec leurs homologues ;
- des outils de gestion du risque informationnel et de gestion de la sécurité ;
- des outils de mise en œuvre de la sécurité qui permettent de développer la confiance dans les applications et services offerts (transactions commerciales et financières, e-santé, e-gouvernement, e-éducation, e-vote …).

A ce titre, le Burkina Faso s'est déjà doté d'un certain nombre de textes législatifs pour promouvoir le développement de l'économie numérique, parmi lesquels :

- la loi n°061-2008/AN du 27 novembre 2008 portant règlementation générale des réseaux et services de communications électroniques au Burkina Faso, ensemble ses modificatifs ;
- la loi n°045-2009/AN du 10 novembre 2009 portant règlementation des services et des transactions électroniques au Burkina Faso ;
- la loi n°011-2010/AN du 30 mars 2010 portant règlementation de la gestion des noms de domaine sous le domaine de premier niveau .bf ;
- la loi n°025-2018/AN du 31 mai 2018 portant code pénal ;
- la loi n°001-2021/AN du 30 mars 2021 portant protection des personnes à l'égard du traitement des données à caractère personnel.

Bien que ces lois constituent un début de solution à la question liée à la sécurité des systèmes d'information, l'état actuel du cadre juridique du Burkina Faso, de manière générale, présente quelques insuffisances en matière de cyber sécurité. Il s'avère donc impérieux d'étoffer le cadre légal et règlementaire pour mieux contrôler et sécuriser le cyberespace national afin de faire face efficacement à toutes les menaces effectives ou potentielles.

Ce cadre légal permettra à l'organe en charge du contrôle et de la protection du cyberespace national d'effectuer certaines missions de contrôle du cyberespace national, notamment l'imposition d'un audit périodique obligatoire des systèmes et actifs numériques, l'obligation de conservation des traces informatiques, la possibilité de sanctionner les acteurs défaillants ou malveillants ainsi que la protection spéciale des organismes à infrastructures critiques pour la souveraineté nationale.

Par ailleurs, une étude relative à l'audit du cadre juridique et proposition de textes législatifs pour encadrer le développement de l'économie numérique commanditée, en mars 2017, par l'Assemblée nationale avec ses partenaires a abouti à la nécessité d'adopter une loi pour régir la sécurité des systèmes d'information du Burkina Faso.

C'est ainsi qu'au regard de ce contexte national et international, le présent projet de loi est proposé pour régir la sécurité des systèmes d'information du Burkina Faso.

I.2. PROCESSUS D'ELABORATION DU PROJET DE LOI

Pour l'élaboration de ce projet de loi, un comité technique interministériel a été mis en place en août 2017.

Ce comité était composé des représentants de la Primature, des Ministères en charge des Finances, de l'Economie numérique, de la Justice, de la Sécurité, de la Défense nationale, du Commerce et des structures telles que l'Agence nationale de promotion des technologies de l'information et de la communication (ANPTIC), l'Autorité de régulation des communications électroniques et des postes (ARCEP), la Commission de l'informatique et des libertés (CIL), l'Agence nationale de sécurité des systèmes d'information (ANSSI) et de personnes ressources du secteur de l'Informatique.

Tout en tenant compte du contexte national et s'inspirant des exigences imposées par les textes nationaux, régionaux et internationaux, le comité a élaboré l'avant-projet de loi qui a été soumis à validation lors d'un atelier national ayant rassemblé, outre les membres du comité, des acteurs venant d'autres ministères et institutions, de la société civile et du secteur privé. Son examen par le Comité technique de vérification des avant-projets de loi (COTEVAL) est intervenu le 25 avril 2018.

A la suite, l'avant-projet de loi a été soumis en Conseil des ministres en novembre 2018 et son examen a abouti à la formulation d'amendements. Le comité d'élaboration s'est réuni à nouveau en août 2021 lors d'un atelier et a pris en compte lesdits amendements.

Cette nouvelle mouture de l'avant-projet de loi a été réexaminée par le COTEVAL le 08 décembre 2021, en vue de s'assurer de l'intégration de l'ensemble des amendements et programmée en Conseil des ministres le 26 Janvier 2022.

Avec les changements institutionnels intervenus au Burkina Faso le 24 janvier 2022, c'est finalement le 22 novembre 2023 que le dossier a été adopté en Conseil des ministres.

Dans les perspectives de sa réintroduction en Conseil des ministres, le dossier a été examiné en Conseil de cabinet, l'une des orientations, outre son appropriation par les acteurs, était d'attendre que le projet de loi portant sécurité nationale soit d'abord adopté avant celui relatif à la sécurité des systèmes d'information, en vue de s'assurer de la cohérence normative entre les deux projets de lois.

Pour ce qui est de l'appropriation de l'avant-projet de texte, une séance de travail entre les équipes techniques de l'ANSSI et du Ministère en charge de la Transition digitale a été tenue le 07 juin 2022 et a permis d'apporter des amendements audit avant-projet.

La mouture actuelle de l'avant-projet de loi est issue de la session du COTEVAL tenue les 8 et 9 décembre 2022 avec la prise en compte des observations antérieures.

Par la suite, deux séances de travail ont été tenues ; la première entre le Ministère en charge de la Transition digitale et l'ANSSI pour s'assurer de la prise en compte des amendements du COTEVAL et la seconde entre les acteurs précités et le Ministère en charge de la Défense pour apprécier la prise en compte de la notion de cyberdéfense par l'avant-projet portant sécurité des systèmes d'information.

I.3. CONTENU DU PROJET DE LOI

Le présent projet de loi comprend quatre (4) titres comportant huit (08) chapitres et trente-quatre (34) articles.

Le titre I, subdivisé en deux (02) chapitres, traite des dispositions générales :

- le chapitre 1 définit l'objet et fixe le champ d'application de la loi ;
- le chapitre 2 porte sur la définition de certains termes techniques employés dans le projet de loi.

Le titre II, subdivisé en trois (03) chapitres, porte sur les dispositions relatives à la sécurisation des systèmes d'information :

- le chapitre 1 est relatif aux orientations générales de la sécurité des systèmes d'information ;
- le chapitre 2 traite du contrôle et de la protection des systèmes d'information ;
- le chapitre 3 évoque les procédures applicables et les conditions attachées aux régimes des accréditations, agréments et homologations.

Le titre III, subdivisé en deux (2) chapitres, est relatif aux obligations et sanctions :

- le chapitre 1 définit les obligations des exploitants des systèmes d'information ;
- le chapitre 2 est relatif aux sanctions encourues en cas de manquement à la règlementation.

Le titre IV traite des dispositions transitoires et finales.

II. DEBAT GENERAL

Au terme de l'exposé de madame le Ministre, les commissaires ont exprimé des préoccupations à travers des questions auxquelles des éléments de réponse leur ont été apportés.

<u>Question n°1</u> : **Dans l'exposé des motifs, à la page 3, il est fait mention de 5 lois relatives au développement de l'économie numérique. Les décrets d'application de ces lois ont-ils été pris ? Ces lois ont-elles connu des débuts d'application ? Avaient-elles des failles ou des faiblesses qui justifient le vote d'une nouvelle loi ?**

<u>Réponse</u> : La plupart des textes d'application de ces lois ont été déjà pris. A titre d'exemple la loi n°001-2021/AN du 30 mars 2021 portant protection des personnes à l'égard du traitement des données à caractère personnel a prévu quatre textes règlementaires dont deux ont été déjà adoptés et un en cours de finalisation. Ils sont relatifs à l'organisation et au fonctionnement de la Commission de l'informatique et des libertés (CIL) et à son règlement intérieur. Celui relatif à la perception des redevances sur les prestations de la CIL est en cours d'élaboration.

D'autres textes ont déjà fait l'objet de modification pour tenir compte des réalités nouvelles. C'est le cas par exemple du code pénal révisé en 2018 qui a pris en compte la criminalisation des cybermenaces.

Les lois citées dans l'exposé des motifs couvrent des parties de la matière sécurité informatique mais pas toute la matière. Au regard de l'importance du sujet, il était important d'élaborer une loi spécifique afin de rendre obligatoire, aux acteurs, certaines dispositions telles que l'audit périodique des systèmes et actifs numériques et la conservation

des traces informatiques en local. Le présent projet de loi permet également de définir des sanctions à l'encontre des contrevenants.

<u>Question n°02</u> : Le projet de loi a-t-il pris en compte les nouvelles avancées dans le domaine du numérique notamment l'Intelligence artificielle ?

<u>Réponse</u> : Le présent projet de loi définit le cadre de la sécurité des systèmes d'information. Les textes d'application et les différents référentiels et cahiers des charges permettront d'adresser toutes les problématiques mêmes celles émergentes et donnera aussi la flexibilité de les adapter aux évolutions.

<u>Question n° 03</u> : Que faut-il entendre par « Système d'information » ? Cette notion est-elle nécessairement liée à internet ?

<u>Réponse</u> : Le Système d'information (SI) est un ensemble de ressources et de dispositifs permettant de collecter, stocker, traiter et diffuser les informations nécessaires au fonctionnement d'une organisation.

Dans son sens large, le Système d'information n'a pas besoin d'être un système numérique et ne doit pas être confondu avec le système informatique qui est un sous ensemble du système informatique regroupant l'ensemble des moyens informatiques nécessaires au traitement de l'information tels que les ordinateurs, programmes, réseaux, logiciels, etc.

Le sens retenu dans ce projet de loi est celui de système d'information numérique.

Un système d'information peut exister sans internet, en ce sens que les équipements informatiques du système d'information peuvent fonctionner sans être connectés à internet.

Cependant, lorsque ce système d'information voudrait échanger avec un autre système d'information distant, internet peut permettre cet échange.

<u>Question n°04</u> : Le Gouvernement peut-il donner une meilleure définition des notions de « métadonnée » et d'« organismes à infrastructures critiques » ?

<u>Réponse</u> :

- Une métadonnée est une « donnée qui fournit de l'information sur une autre donnée ». Il s'agit en fait des renseignements qui sont générés

lorsqu'on utilise la technologie et qui permettent de situer diverses activités dans leur contexte (qui, quoi, où, quand et comment).
Par exemple les coordonnées géographiques avec lesquelles les photographies numériques sont étiquetées sont des métadonnées.

- Organisme à infrastructures critiques : c'est un organisme dont les installations, ouvrages et systèmes qui sont indispensables au maintien des fonctions vitales de la société et qui contribuent fortement à la santé, à la sûreté, à la sécurité et au bien-être économique ou social et dont le dommage, l'indisponibilité ou la destruction aurait un impact induisant la défaillance de ces fonctions.

<u>Question n°05</u> : A l'article 5 du présent projet de loi, il est question d'un organe de contrôle et de protection du cyberespace national. Cet organe ne va-t-il pas être un doublon de l'Agence nationale de sécurité des systèmes d'information (ANSSI) ?

<u>Réponse</u> : Dans l'entendement du Gouvernement, les missions de l'organe national en charge du contrôle et de la protection du cyberespace sont celles assurées par l'ANSSI déjà créée par voie règlementaire. C'est dans un souci de flexibilité et pour garder le caractère général du présent projet de loi que l'ANSSI n'a pas été nommée comme étant l'organe national évoqué.

<u>Question n°06</u> : A l'article 26 du projet de loi, pour les manquements d'un organisme relatif à des activités d'importation et de vente, il est question d'un délai de mise en demeure qui ne doit pas excéder 24 mois. Ce délai n'est-il pas trop long au vu de l'infraction ?

<u>Réponse</u> : Ce délai peut effectivement sembler long au premier abord. Il faudra noter qu'il s'agit d'un délai maximal. Toutefois, il vise à permettre aux organismes de disposer du temps pour répondre aux manquements de manière complète, en tenant compte de la complexité potentielle des ajustements réglementaires ou opérationnels nécessaires. Cependant, la durée pourrait effectivement être moindre pour des infractions particulièrement graves ou urgentes, afin de garantir une réponse plus rapide et efficace qui corresponde mieux à la gravité de l'infraction.

<u>Question n°07</u> : A l'article 5 du présent projet de loi, il est question de contrôle et de protection des systèmes d'information. En quoi consiste cette protection ?

Réponse : La protection consiste à faire usage de mesures techniques, organisationnelles, légales et administratives pour prévenir, détecter les menaces ou risques ou alors corriger ou rétablir le système suite à un incident impactant des services ou des équipements.

Question n°8 : L'article 13 du présent projet de loi dispose que « les exploitants des systèmes d'information ont l'obligation de conserver au Burkina Faso les métadonnées de connexion et de trafic de leur système d'information pendant une période de 3 ans minimum ». Est-ce à dire qu'ils ont l'obligation d'héberger leur serveur au Burkina Faso ?

Réponse : Il est important de distinguer l'hébergement des données opérationnelles et la conservation des métadonnées. Même si les données opérationnelles peuvent être hébergées à l'étranger, les métadonnées, qui sont essentielles pour les enquêtes de sécurité et les audits, doivent être conservées localement pour garantir qu'elles restent accessibles pour les autorités compétentes, conformément à la législation nationale.

De plus, l'article 13, alinéa 9 du projet de loi, précise que dans les cas où il serait techniquement impossible de conserver les métadonnées localement, celles-ci doivent alors être stockées selon des normes de sécurité strictes définies par l'organe national chargé de la protection du cyberespace.

Question n°9 : Le Gouvernement a-t-il la certitude que tous les exploitants des systèmes d'information conservent au Burkina Faso les métadonnées de connexion et de trafic ?

Le Gouvernement a-t-il la certitude que tout le monde le fait ?

Cette loi permettra-t-elle au Gouvernement d'avoir les moyens de s'en assurer ?

Réponse : À date, il n'existe pas de textes législatifs ou règlementaires obligeant les acteurs à conserver les métadonnées durant une période déterminée. L'adoption du présent projet de loi introduira une telle obligation aux acteurs identifiés dans le présent projet de loi.

Aussi, il convient de noter que le choix d'exiger la conservation des métadonnées et non toutes les données se justifie par le fait de rendre cette obligation facile à respecter pour les acteurs et à contrôler par l'organe chargé de la protection du cyberespace national.

<u>Question n°10</u> : Que doit-on entendre par « incident de sécurité à impact critique » ? Y a-t-il une cartographie de ces incidents ?

<u>Réponse</u> : Un « incident de sécurité à impact critique » désigne tout événement anormal dans le fonctionnement du Système d'information (SI) qui peut, ou a déjà gravement perturbé les opérations essentielles d'une organisation ou de structures critiques au bon fonctionnement de la nation. Cela inclut les incidents qui, par leur ampleur, affectent des systèmes d'information sensibles et peuvent paralyser significativement, voire totalement, les activités concernées.

Les conséquences d'un tel incident peuvent être diverses, allant de lourdes pertes financières et matérielles à des dommages significatifs pour la réputation de l'entité, une interruption prolongée des services, voire, dans des cas extrêmes, des pertes de vies humaines.

Sur le plan de la classification, les incidents de sécurité sont généralement évalués selon des critères internationalement reconnus qui les rangent en trois niveaux de gravité : bas, moyen et élevé. Cette classification est fondée sur l'impact potentiel ou réel de l'incident en termes de conséquences négatives pour l'organisation.

Concernant la cartographie des incidents, il existe effectivement un document qui recense ces événements selon leur criticité. Toutefois, ce document nécessite une mise à jour régulière pour refléter l'évolution des menaces et des vulnérabilités dans le cyberespace, ainsi que l'émergence de nouveaux types d'incidents critiques. Cela permet aux organismes concernés et à l'Autorité de régulation de mieux préparer et ajuster leurs stratégies de réponse aux incidents.

<u>Question n°11</u> : A l'article 19 du présent projet de loi, dernier alinéa, il est écrit que « *L'organisme peut, en outre, être contraint de déconnecter son système d'information du réseau national et international ou être interdit d'exercer son activité pendant une durée fixée par l'organe national en charge du contrôle et de la protection du cyberespace national.* » De quels moyens dispose l'Etat pour le contraindre à se déconnecter du réseau international ?

Réponse : L'État peut recourir à :

- des mécanismes pour bloquer l'accès aux réseaux internationaux. Cela peut être réalisé par la coopération avec les fournisseurs de services internet qui peuvent techniquement limiter ou couper l'accès aux services concernés.

- la collaboration entre l'organe national en charge du contrôle et de la protection du cyberespace national et les autres agences gouvernementales telles que les autorités de régulation des télécommunications et les forces de l'ordre, pour assurer l'application de ces mesures.

Ces moyens, soutenus par la loi, garantissent que l'État possède les outils nécessaires pour faire respecter des mesures drastiques en cas de nécessité impérieuse liée à la sécurité des systèmes d'information et la protection du cyberespace national.

Question n°12 : Quels sont les moyens, outils ou équipement dont dispose l'Etat pour contrôler et protéger notre cyberespace national ?

Réponse : Pour contrôler et protéger notre cyberespace national, l'État, à travers Agence nationale de sécurité des systèmes d'information (ANSSI), la Brigade centrale de lutte contre la cybercriminalité (BNVAA), Brigade numérique de veille d'alerte et d'assistance (BCLCC), la Direction centrale des systèmes d'information et de la cyberdéfense (DCSIC), l'Agence nationale de renseignement (l'ANR) dispose de plusieurs ressources stratégiques qui forment un dispositif de défense pour contrer les menaces cybernétiques. Ces moyens comprennent :

1. les ressources humaines : personnel hautement qualifié dans le domaine de la cybersécurité bien que le besoin de renforcement de l'expertise nationale en quantité et en qualité demeure un défi ;

2. les moyens juridiques : un cadre réglementaire complet, incluant des lois, des décrets et des arrêtés ainsi que l'adoption de normes internationales qui régissent la sécurité des systèmes d'information et la réponse aux cyberattaques ;

3. les capacités organisationnelles : des structures spécialisées telles que l'ANSSI, ayant de missions claires et travaillant en synergie pour une réponse coordonnée à l'échelle nationale ;

4. les canaux de coopération : des accords de collaboration aussi bien au niveau national qu'international, permettant un échange efficace d'informations sur les menaces et les meilleures pratiques en matière de cybersécurité ;
5. les moyens techniques : des infrastructures techniques avancées, incluant des centres opérationnels de sécurité (SOC), des équipes de réponse aux incidents informatiques (CIRT) et des technologies pour inspecter et sécuriser le matériel connecté au réseau national. Ces outils sont essentiels pour détecter, prévenir et répondre aux incidents de sécurité.

<u>Question n°13</u> : A l'article 24 du projet de loi, pourquoi l'interdiction d'exercer ne doit pas excéder 12 mois ? Quelle est la durée de la suspension ?

<u>Réponse</u> : Cette mesure temporelle vise à maintenir un équilibre entre la nécessité de punir et de corriger les non-conformités, tout en permettant à l'entité de prendre les mesures correctives nécessaires et de reprendre ses activités, si elle démontre une amélioration substantielle de sa conformité.

Concernant la durée de la suspension, elle n'est pas spécifiquement définie dans l'article pour permettre une flexibilité dans l'application de la loi. Cela prend en compte le fait que les manquements peuvent varier considérablement en termes de gravité et d'impact. La durée exacte de la suspension pourra être déterminée en fonction des circonstances spécifiques de chaque cas et sera précisée dans les textes d'application. Cela permettra une adaptation aux divers contextes et de s'assurer que les sanctions sont proportionnelles à la nature et à la gravité du manquement.

<u>Question n°14</u> : Quel type de collaboration va-t-on avoir entre l'organe en charge de la protection du cyberespace national et la structure logée au sein du Ministère de la Défense ?

<u>Réponse</u> : L'article 30 du projet de loi prévoit une collaboration étroite entre l'organe national en charge de la protection du cyberespace et la structure dédiée au sein du Ministère de la Défense. Cette collaboration se manifestera principalement à travers des échanges d'informations et d'expertises sur les menaces et les incidents de sécurité cybernétique.

<u>Question n°15</u> : Quel est le niveau de certification demandé au Burkina Faso ?

<u>Réponse</u> : Le présent projet de loi ne définit pas explicitement un niveau minimal de certification pour la sécurité des systèmes d'information. Toutefois, les exploitants des systèmes d'information devraient appréhender et adhérer aux principes du Référentiel général de sécurité du Burkina Faso (RGS-BF), qui établit des standards de sécurité à respecter.

Les audits réglementaires, prévus par le présent projet de loi, permettront d'évaluer la conformité des systèmes d'information à ces standards et déterminer si les exploitants maintiennent un niveau de sécurité adéquat.

<u>Question n°16</u> : Etant donné que les innovations et les menaces évoluent très vite, les certificats doivent être révisés de façon périodique ; est-ce effectif dans notre pays ?

<u>Réponse</u> : La révision des certificats est effectivement mise en œuvre au Burkina Faso. Elle est régulée par des mécanismes de gestion des certificats.

L'organe national chargé de la protection du cyberespace dispose de systèmes automatisés pour surveiller la validité des certificats. Ces systèmes détectent non seulement les certificats expirés mais aussi ceux susceptibles d'être compromis ou révoqués avant la fin de leur période de validité prévue. En cas de détection d'une anomalie ou d'une vulnérabilité, une intervention rapide est déclenchée pour réémettre ou mettre à jour le certificat concerné.

<u>Question°17</u> : Comment obtenir l'accréditation dont il est question à l'article 7 du présent projet de loi ?

<u>Réponse</u> : Les conditions d'obtention de l'accréditation seront précisées par le décret d'application prévu à l'article 6 du présent projet de loi.

<u>Question n°18</u> : La confidentialité liée aux données est-elle limitée dans le temps ?

<u>Réponse</u> : La confidentialité des informations n'est généralement pas limitée dans le temps. Cependant, la durée pendant laquelle les données doivent rester confidentielles dépend souvent du type de données et des exigences réglementaires ou contractuelles spécifiques.

<u>Question n°19</u> : Au niveau de l'article 8 du présent projet de loi, il est question d'un audit qui doit se faire tous les 2 ans ; ne faut-il pas plutôt un audit annuel pour les structures sensibles ?

Réponse : Les entités jugées essentielles pour la sécurité nationale et la continuité des services publics doivent être officiellement désignées par l'État burkinabè sous l'appellation d'Organismes à infrastructures critiques (OIC). Ces OIC sont soumis à un cadre réglementaire plus strict, incluant des plans de protection spécifiques et renforcés.

Conformément aux dispositions de l'article 15 du présent projet de loi, la nature et la périodicité des audits de ces structures seront déterminées par décret. Cette disposition offre la flexibilité nécessaire pour adapter la fréquence des audits en fonction de l'évolution des menaces et des besoins de sécurité, permettant ainsi une réponse plus agile et ciblée aux risques potentiels.

Question n°20 : Au niveau de l'article 9 du présent projet de loi, le Gouvernement peut-il définir clairement le temps qu'il faut avant la levée du secret confidentiel ?

Réponse : L**e** secret professionnel, par nature, n'a pas de limite.

Question n°21 : En matière de cyberattaque et de cybercriminalité, les situations doivent être prises immédiatement en charge ; le délai de 48 heures pour la transmission après constat n'est-il pas trop long ?

Réponse : Un délai de 48 heures pour notifier un incident de cybersécurité est retenu pour permettre aux responsables de la gestion des incidents de mener les analyses forensiques nécessaires. Ce délai est calibré pour équilibrer la rapidité de la réaction et l'exactitude de l'analyse, pour assurer une réponse efficace à l'incident tout en contribuant à la prévention de futurs incidents dans un cadre collaboratif.

Question n°22 : Le Gouvernement peut-il justifier l'absence de sanction privative de liberté dans le présent projet de loi ?

Réponse : Les sanctions privatives de liberté sont déjà prévues dans le code pénal révisé de 2018. L'organe national en tant qu'organe non juridictionnel n'est pas habilité à prononcer des sanctions privatives de liberté.

<u>Question n°23</u> : Comment le présent projet de loi se positionne par rapport à la législation en matière de sécurisation des systèmes d'information dans la sous-région ?

<u>Réponse</u> : Le présent projet de loi s'est inspiré des lois existantes au plan régional et international (Cameroun, Tunisie, Maroc, France). Il s'est également inspiré des Conventions de Malabo et de Budapest.

<u>Question n°24</u> : Le Burkina Faso a-t-il la maîtrise des frontières d'Internet de son territoire ?

<u>Réponse</u> : Pour l'instant, bien que notre pays ne maîtrise pas intégralement les frontières d'Internet, il a déjà mis en place une supervision de certaines de ses connexions internationales ainsi que de diverses infrastructures étatiques. De plus, plusieurs projets sont actuellement en cours pour renforcer cette capacité à superviser toutes les sorties Internet.

Concernant les VPN, il est important de reconnaître que même des nations développées rencontrent des difficultés similaires. Par exemple, la Chine a des défis avec le blocage de Facebook. Cependant, le renforcement du plateau technique permettra de bloquer les adresses IP utilisées par ces technologies.

En ce qui concerne spécifiquement les équipements de communication par satellite, l'action coordonnée des différents acteurs parties prenantes permet de réguler ce sous domaine et prendre les dispositions appropriées.

<u>Question n°25</u> : Au niveau de l'article 6 du présent projet de loi, pourquoi se limiter à l'importation et à la vente ? Qu'en est-il des outils conçus et développés localement ?

<u>Réponse</u> : Pour les outils conçus et développés localement, ils seront concernés dès lors qu'ils sont destinés à la vente. Cet article, bien que visant essentiellement les produits destinés à la commercialisation, s'applique également aux produits locaux ayant la même finalité.

<u>Question n° 26</u> : Quel est le degré de menace de la sécurité de l'information dans notre pays ?

Le degré de menace de la sécurité de l'information d'un pays peut être évalué à travers plusieurs indicateurs clés, révélateurs de la prévalence des cybermenaces et des vulnérabilités des systèmes nationaux. Au

regard de l'évolution des valeurs de ces indicateurs, le degré de menace en matière de sécurité des systèmes d'information du Burkina Faso peut être qualifié d'élevé.

<u>Question n° 27</u> : Le Gouvernement peut-il indiqué à la représentation nationale le niveau de vulnérabilité de notre système d'information ?

<u>Réponse</u> : Le niveau de vulnérabilité des systèmes d'information est apprécié suivant un certain nombre de rapports d'attaques ou du respect de certaines dispositions. L'examen de ces éléments d'appréciation permet de qualifier d'élevé le niveau de vulnérabilité de notre système d'information.

<u>Question n°28</u> : Peut-on avoir le bilan des projets mis en œuvre sur les systèmes d'information, l'hébergement des données et le contrôle de l'internet ?

<u>Réponse</u> : Le Burkina Faso a mis en œuvre des projets de développement d'infrastructures de communication et d'hébergement ainsi que des plateformes numériques. Au titre de ces projets, il y a le Projet régional ouest-africain d'infrastructures de communication (PRICAO), le projet cloud gouvernement (GCloud), le Projet Backbone national de télécommunication (PBNT), le Projet d'appui au développement des technologies de l'information et de la communication (PADTIC), le projet eBurkina. Ci-dessous, une synthèse de l'état de mise en œuvre de ces projets :

- le PRICAO a permis de mailler le territoire en Fibre optique (FO) pour raccorder les régions avec 335 Km ;

- le GCloud a permis de mettre en place un datacenter cloud avec 8 nœuds dont 4 à Ouaga et 4 à Bobo au profit de l'Administration publique. Au total 591 Km de FO ont été posés pour raccorder des chefs de lieu de région et les nœuds du datacenter national au RESINA ;

- le PBNT a permis de réaliser le Backbone national avec 2085 Km de Fibre optique posés pour interconnecter les chefs-lieux de région ;

- le PADTIC a permis de mettre en place des infrastructures de communication dont 3 stations satellitaires (non fonctionnelles aujourd'hui pour cause de coûts récurrents non-supportables par l'État) et d'énergie et l'aménagement de réseaux locaux ;

- le projet eBurkina a permis de développer des infrastructures, des plateformes numériques et de renforcer les capacités et les compétences des acteurs de l'écosystème du numérique.

Pour l'ensemble de ces projets, au total 157 656 395 499 FCFA ont été mobilisés et 154 700 046 392 FCFA ont été exécutés avec les taux d'exécution physique et financière globaux respectifs de 97,03% et de 98,12%.

<u>Question n°29</u> : Existe-t-il ou est-il envisagé la mise en place d'un Etat-major en matière de cyberdéfense au Burkina Faso ?

<u>Réponse</u> : Face à l'avancée et à la diversité des cybermenaces, la création d'un État-major en matière de cyberdéfense au Burkina Faso est une nécessité. Elle est une préoccupation déjà prise en charge au niveau du Ministère de la Défense. Une synergie d'actions entre les différentes parties-prenantes est indispensable.

<u>Question n°30</u> : Que renferme le terme « Economie numérique » ?

<u>Réponse</u> : Le terme « Economie numérique » est l'ensemble des activités relatives aux Technologies de l'information et de la communication (TIC), à la production et à la vente de produits et services numériques.

<u>Question n°31</u> : Quelle est la limite du cyberespace national ?

<u>Réponse</u> : Le cyberespace d'un pays est généralement défini comme l'ensemble des ressources informatiques connectées géographiquement à l'intérieur de ce pays ainsi que les ressources appartenant à ce pays mais hébergées à l'extérieur. Cette définition pose une limite claire : le contrôle et la maîtrise des ressources informatiques au-delà des frontières nationales sont réduits.

<u>Question n°32</u> : Quel est l'impact financier de la mise en œuvre de la loi ?

<u>Réponse</u> : Les projections prévisionnelles pour la mise en œuvre de la loi si elle est adoptée donnent un budget prévisionnel de 60 milliards de FCFA destinés à renforcer le dispositif technique de supervision, d'audit et les capacités humaines et matérielles.

<u>Question n°33</u> : Le Gouvernement peut-il exposer les grandes menaces de notre système ?

<u>Réponse</u> : Le Burkina Faso fait face à un degré de menace élevé en matière de sécurité de l'information, marqué par une prévalence élevée de systèmes infectés (8 212 pour 100 000 utilisateurs), un nombre important de vulnérabilités (1 435 pour 100 000 utilisateurs), des ports ouverts non utilisés (44 pour 100 000 utilisateurs) et des comportements utilisateurs à risque (3 875 pour 100 000 utilisateurs). Les plaintes pour cybercriminalité ont également augmenté, passant de 602 en 2020 à 3 954 en 2023.

<u>Question n°34</u> : Quel est le dispositif de gestion du risque mis en place ?

<u>Réponse</u> : Le dispositif de gestion des risques mis en place comprend plusieurs aspects :

- la supervision des SI par le Security operation center (SOC) et extension de cette supervision à toutes les entrées et sorties internet ;
- le renforcement du plateau technique de gestion des incidents qui facilitera les échanges d'informations sur les menaces ;
- le RGS-BF qui définit le processus de gestion des risques (normes et méthodologie) ;
- les scans de vulnérabilités et audit qui sont menés sur le terrain.

De plus, le présent projet de loi viendra rendre obligatoire les audits périodiques ainsi que l'homologation des équipements et logiciels qui seront utilisés dans les systèmes critiques. Toutes ces dispositions devront permettre de réduire considérablement le risque qui pèse sur notre cyberespace.

<u>Question n°35</u> : La première phrase du dernier alinéa de l'article 8 du présent projet de loi dispose que : *« La liste des matériels et de logiciels concernés ainsi que les organismes sont déterminés par voie règlementaire* ». Existe-il une liste nominative de ce matériel et de ces logiciels ? Si non, comment cette liste sera-t-elle opérationnelle ?

<u>Réponse</u> : Cette liste n'est pas encore formellement établie. Avec le présent projet de loi, elle sera formalisée de concert avec les autres acteurs et mise à

jour régulièrement par voie règlementaire. Une catégorisation est proposée dans le projet de décret joint au projet de loi.

<u>Question n°36</u> : Au niveau de l'article 13 du présent projet de loi, les organismes assujettis sont-ils à mesure de respecter toutes les obligations énoncées ?

<u>Réponse</u> : L'importance de la question de sécurité des systèmes d'information exige de leur part qu'ils prennent les mesures nécessaires pour assurer la protection de tout ce qui est sensible et de contribuer par conséquent à la protection du cyberspace national.

<u>Question n°37</u> : Au regard du champ d'application de la présente loi et des prérogatives qu'elle accorde à l'organe chargé du contrôle en matière de sanctions, n'y a-t-il pas un empiètement sur les attributions de l'ARCEP ?

<u>Réponse</u> : Il n'y a pas d'empiètement car le champ d'action de l'ARCEP concerne la régulation des communications électroniques alors que le présent projet de loi traite de la sécurité des systèmes d'information.

<u>Question n°38</u> : Quels seront le rôle et la place de la Brigade de lutte contre la cybercriminalité (BCLCC) aux côtés de la structure nationale ?

<u>Réponse</u> : La sécurisation des systèmes d'information englobe à la fois la cybersécurité, la cybercriminalité et la cyberdéfense. Il y a donc pour chaque pan des acteurs avec des missions et attributions déjà définies. Les actions de ces différents acteurs sont complémentaires.

<u>Question n°39</u> : La constatation des manquements évoqués dans le projet de loi ressemble bien à des actes de police judiciaire. Est-ce que les acteurs chargés d'animer la structure nationale en charge du contrôle et de la protection du cyberespace auront la qualité d'officier de police judiciaire ?

<u>Réponse</u> : Les constatations de manquements sont faites selon des procédures d'audit bien définies. Ne pas avoir la qualité d'Officier de police judiciaire (OPJ) n'est pas un facteur bloquant. De plus, la collaboration avec les autres entités permet à celles ayant cette qualité d'agir en cas de besoin.

Question n°40 : Les obligations prévues à l'article 13 du présent projet de loi s'appliquent-elles aux exploitants nationaux. Dans l'affirmative, ces exploitants pourront-ils respecter ces obligations ?

Réponse : Les obligations concernent tous les exploitants et, par conséquent, même les nationaux ont l'obligation de s'y conformer.

Question n°41 : Le délai de trois ans fixés à l'article 13, 1er tiret du présent projet de loi, n'est-il pas de trop ?

Réponse : Le délai de trois (03) ans n'est pas de trop parce que ces données doivent servir pour les investigations en cas de manquement.

Question n°42 : Le présent projet de loi porte sécurité des systèmes d'information au Burkina Faso. Que vaut le présent projet de loi si nos bases de données continuent d'être hébergées à l'extérieur ?

Réponse : Les bases de données hébergées à l'extérieur constituent une préoccupation prise en considération par le Gouvernement. Des projets déjà en cours devront très bientôt permettre de disposer d'infrastructures d'hébergement permettant d'exiger l'hébergement en local des données sensibles.

Question n°43 : Le Burkina Faso a-t-il déjà été victime d'attaque ou de vol de ces données ? Si oui, quelle en a été l'ampleur ?

Réponse : De nombreux cas ont été enregistrés pour ce qui concerne le Burkina Faso. C'est le cas par exemple de sites de médias nationaux ou des infrastructures de certaines institutions. Dans la plupart des cas, il y a une atteinte à la réputation, une perte significative de données, un temps prolongé d'arrêt de production et des pertes financières importantes dues aux efforts de rétablissement du système.

Question n°44 : Le Gouvernement peut-il faire à la Représentation nationale l'état du matériel de communication détruit par les terroristes ?

Réponse : Au total 201 sites de pylônes ont été vandalisés par les terroristes, tous opérateurs confondus (Moov, Telecel, ANPTIC et Orange). Les opérateurs travaillent à rétablir les sites vandalisés avec l'accompagnement des forces de défenses et de sécurité souvent au prix de la vie de leurs travailleurs. Le Gouvernement qui suit de près cette situation a mobilisé des ressources financières dans le cadre des mesures

d'urgence pour accompagner le rétablissement des sites détruits dans les zones à haut défi sécuritaire.

Il faut cependant noter que ces statistiques évoluent suivant la dynamique de la reconquête du territoire.

Question n°45 : Existe-t-il une synergie d'actions entre les différentes structures en charge de la sécurité des systèmes d'information ? Si non, n'y a-t-il pas nécessité de formaliser un cadre, pour ces structures, de mutualisation de leurs actions ?

Réponse : Dans le cadre de la mise en œuvre de la stratégie nationale de cybersécurité du Burkina Faso, il existait un conseil national de suivi de cette stratégie nationale en cybersécurité. Ce conseil regroupait les acteurs clés de l'écosystème du numérique.

A travers un réseau de points focaux mis en place au niveau des Directions des systèmes d'information, l'ANSSI collabore étroitement avec ses dernières en vue de les accompagner dans la sécurisation des systèmes d'information sectoriels.

Par ailleurs, des conventions existent notamment entre l'ANSSI et certaines entités telles que la CIL et la BCLCC.

Enfin, le présent projet de loi prévoit un cadre de concertation formalisé entre les différents acteurs pour plus de synergie et d'efficacité dans la sécurisation du cyberespace national.

Question n°46 : N'y a-t-il pas nécessité, pour plus d'efficacité, d'associer les autres structures du secteur de l'informatique au processus d'accréditation par l'Agence nationale de sécurité des systèmes d'information (ANSSI) ?

Réponse : Les processus d'accréditation sont généralement gérés par des comités pouvant faire appel à la contribution de plusieurs structures et de personnes de ressources. Les structures proposées pourront être associées dans ce sens en temps opportun.

Question n°47 : Le Gouvernement peut-il clarifier les dispositions de l'article 10 du projet de loi sur le secret professionnel et le secret des affaires ? A qui se rapporte la « personne régulièrement commise pour l'assister ou le conseiller » dans le premier alinéa de l'article 10 du présent projet de loi ?

Réponse : Le secret professionnel est le secret qu'une personne doit garder sur toute information dont elle a eu connaissance dans l'exercice de ses fonctions et qu'elle doit tenir caché soit qu'il lui a été demandé, soit qu'il est inhérent à la nature du fait. La confidentialité dont il est question ne renvoie pas à la clarification de l'information qui relève du secret d'Etat. Il n'y a donc pas de durée à déterminer.

Question n°48 : A quoi renvoie l'urgence dont il est fait mention à l'article 28 du projet de loi ?

Réponse : En cas d'urgence, l'organe national en charge du contrôle et de la protection du cyberespace national prend toutes les mesures conservatoires qu'il juge nécessaires

L'urgence ici renvoie à la possibilité qu'il y ait une situation exceptionnelle qui nécessite des actions immédiates pendant la période transitoire et cela sera fait par l'organe en charge de la protection du cyberespace national.

L'urgence dans cet article fait référence à tout incident de sécurité à impact critique. A cet effet, l'organe pourrait prendre toutes les dispositions nécessaires pour limiter les dommages de l'incident.

III. EXAMEN DU PROJET DE LOI ARTICLE PAR ARTICLE

A l'issue du débat général, les commissaires ont procédé à l'examen du projet de loi article par article et y ont apporté des amendements intégrés au texte issu de la Commission.

IV. APPRECIATION DE LA COMMISSION

La Commission du développement durable estime que l'adoption du présent projet de loi permettra de doter notre pays d'infrastructures informationnelles plus fiables et mieux sécurisées, d'un cadre législatif et institutionnel adapté aux nouvelles menaces, d'un cadre juridique dans le domaine du numérique et de nouvelles perspectives pour :

- améliorer la gouvernance, dynamiser l'économie, mettre en œuvre des services sociaux de base et créer l'emploi ;

- mieux contrôler et sécuriser le cyberespace national afin de faire face à toutes les menaces effectives ou potentielles ;

- contrôler et protéger les systèmes d'information ;

- identifier et gérer les risques et incidents relatifs à la sécurité des systèmes d'information ;

- réduire au minimum les conséquences des incidents de sécurité des systèmes d'information ;

- régir les acteurs intervenant dans la sécurisation des systèmes d'information.

Par conséquent, elle recommande à la plénière l'adoption du présent projet de loi.

Toutefois, la Commission recommande :

- la montée en capacité dans les meilleurs délais des acteurs en charge de la sécurisation du cyberespace national ;
- la sensibilisation des utilisateurs et des administrateurs sur la cybersécurité ;
- une diligence dans l'adoption des textes d'application de la présente loi.

Ouagadougou, le 02 juillet 2024

Le Président

Moussa KONE

Le Rapporteur

Aboubacar KABRE

SEANCE D'APPROPRIATION DU LUNDI 10 JUIN 2024

LISTE DE PRESENCE DES DEPUTES

N° D'ORDRE	NOM ET PRENOM (S)	GROUPE CONSTITUE
1.	KONE Moussa	OSC
2.	TUINA Kanibè	PDCE
3.	SIDIBE Mariam	PP
4.	HIEN Diédon Alain	OSC
5.	DAMIEN/YOUL Ini Inkouraba	FVR
6.	BONZI Nonyeza	FVR
7.	KABRE Kalifa	FVR
8.	KABRE Aboubacar	PDCE
9.	ZONGO Kiswendsida Evariste	PDCE
10.	ZONGO Sayouba	PDCE
11.	NIGNAN Dida	FDS
12.	SAWADOGO Isidore Tégwendé	FDS

LISTE DE PRESNCE DU PERSONNEL

N° D'ORDRE	NOM ET PRENOM (S)	QUALITE
1.	BAYALA Cyrille	Conseiller technique du PALT auprès de la CDD
2.	BASSOLE A. Prosper	Administrateur parlementaire
3.	HIEN/WEDRAOGO Prisca	Administrateur parlementaire
4.	KAMBIRE B. Albert	Administrateur parlementaire
5.	OUEDRAOGO/OUEDRAOGO Aimée Edwige	Administrateur parlementaire
6.	BARRO/OUEDRAOGO Habibou W.	Secrétaire de direction
7.	OUEDRAOGO Nestor	Agent de liaison

SEANCE D'AUDITION DES ACTEURS DU MARDI 11 JUIN 2024

LISTE DE PRESENCE DES DEPUTES

N° D'ORDRE	NOM ET PRENOM (S)	GROUPE CONSTITUE
1.	KONE Moussa	OSC
2.	TUINA Kanibè	PDCE
3.	SIDIBE Mariam	PP
4.	HIEN Diédon Alain	OSC
5.	DAMIEN/YOUL Ini Inkouraba	FVR
6.	BONZI Nonyeza	FVR
7.	KABRE Kalifa	FVR
8.	KABRE Aboubacar	PDCE
9.	ZONGO Kiswendsida Evariste	PDCE
10.	ZONGO Sayouba	PDCE
11.	NIGNAN Dida	FDS
12.	SAWADOGO Isidore Tégwendé	FDS

LISTE DE PRESENCE DES COMMISSIONS SAISIES

N° D'ORDRE	NOM ET PRENOM (S)	COMMISSION
1.	KOMBASSERE Jean Marie	CAGIDH
2.	OUEDRAOGO/COMPAORE Sabine	CAEDS
3.	TAPSOBA Issaka	COMFIB

LISTE DE PRESENCE DU PERSONNEL

N° D'ORDRE	NOM ET PRENOM (S)	QUALITE
1.	BAYALA Cyrille	Conseiller technique du PALT auprès de la CDD
2.	BASSOLE A. Prosper	Administrateur parlementaire
3.	HIEN/WEDRAOGO Prisca	Administrateur parlementaire
4.	KAMBIRE B. Albert	Administrateur parlementaire
5.	OUEDRAOGO/OUEDRAOGO Aimée Edwige	Administrateur parlementaire
6.	BARRO/OUEDRAOGO Habibou W.	Secrétaire de direction
7.	OUEDRAOGO Nestor	Agent de liaison

LISTE DE PRESENCE DES ACTEURS

Structure : LIGUE DES CONSOMMATEURS DU BURKINA FASO (LCB)

(**Absent**)

Structure : ASSOCIATION YAMPUKRI

(**Absent excusé**, mais fera des propositions)

Structure : FED-NUMERIQUE

N° D'ORDRE	NOM ET PRENOM (S)	FONCTION
1.	KARAMBIRI Daniel S.	Président OHB/Membre de la FED Numérique
2.	ROUAMBA Halidou	Président ARCDESI/Fed Numérique

Structure : ISOC-BF

N° D'ORDRE	NOM ET PRENOM (S)	FONCTION
1.	SAWADOGO Zakaria	Vice-président

<u>Structure</u> : EXPERTS

N° D'ORDRE	NOM ET PRENOM (S)	FONCTION
1.	COULIBALY Drissa	Ingénieur informaticien développeur
2.	DAH S. Alfred	Spécialiste en sécurité informatique

SEANCE D'AUDITION DES ACTEURS DU MERCREDI 12 JUIN 2024

N° D'ORDRE	NOM ET PRENOM (S)	GROUPE CONSTITUE
1.	KONE Moussa	OSC
2.	TUINA Kanibè	PDCE
3.	SIDIBE Mariam	PP
4.	HIEN Diédon Alain	OSC
5.	DAMIEN/YOUL Ini Inkouraba	FVR
6.	BONZI Nonyeza	FVR
7.	KABRE Kalifa	FVR
8.	KABRE Aboubacar	PDCE
9.	ZONGO Kiswendsida Evariste	PDCE
10.	ZONGO Sayouba	PDCE
11.	NIGNAN Dida	FDS
12.	SAWADOGO Isidore Tégwendé	FDS

LISTE DE PRESENCE DES COMMISSIONS SAISIES POUR AVIS

N° D'ORDRE	NOM ET PRENOM (S)	COMMISSION
1.	KOMBASSERE Jean Marie	CAGIDH
2.	OUEDRAOGO/COMPAORE Sabine	CAEDS
3.	TAPSOBA Issaka	COMFIB

LLISTE DE PRESENCE DU PERSONNEL

N° D'ORDRE	NOM ET PRENOM (S)	QUALITE
1.	BAYALA Cyrille	Conseiller technique du PALT auprès de la CDD
2.	BASSOLE A. Prosper	Administrateur parlementaire
3.	HIEN/WEDRAOGO Prisca	Administrateur parlementaire
4.	KAMBIRE B. Albert	Administrateur parlementaire
5.	OUEDRAOGO/OUEDRAOGO Aimée Edwige	Administrateur parlementaire
6.	BARRO/OUEDRAOGO Habibou W.	Secrétaire de direction
7.	OUEDRAOGO Nestor	Agent de liaison
8.	BAMOGO Jérôme	Administrateur parlementaire/CAEDS

N° D'ORDRE	NOM ET PRENOM (S)	QUALITE
9.	KYERE/YAOGO D. Téné Pascaline	Administrateur parlementaire/CAGIDH
10.	TINDANO/ZOUNDI Louise	Administrateur parlementaire/COMFIB

LISTE DE PRESENCE DES ACTEURS

Structure : CONSEIL SUPERIEUR DE LA COMMUNICATION

N° D'ORDRE	NOM ET PRENOM (S)	FONCTION
1.	OUEDRAOGO Amadou Lamine	Directeur informatique

Structure : COMMISSION DE L'INFORMATIQUE ET DES LIBERTES (CIL)

N° D'ORDRE	NOM ET PRENOM (S)	FONCTION
1.	NASSA/TRAWINA Haliguiéta	Présidente
2.	K-NION/SANOU W. Edith	Directrice de Cabinet
3.	BANDE Amidou	Secrétaire général
4.	DA Sié Maxime	Conseiller technique
5.	DIALLA Ousséni	CE

Structure : DIRECTION GENERALE DE L'AGENCE NATIONALE DE RENSEIGNEMENTS (ANR)

(Absent)

Structure : DIRECTION GENERALE DE L'AUTORITE DE REGULATION DES COMMUNICATIONS ELECTRONIQUES ET DES POSTES (ARCEP)

N° D'ORDRE	NOM ET PRENOM (S)	FONCTION
1.	SAVADOGO Yassia	DSI
2.	TETEGAN Lamoussa	DAJ

Structure : DIRECTION GENERALE DE L'AGENCE NATIONALE DE PROMOTION DES TIC (ANPTIC)

N° D'ORDRE	NOM ET PRENOM (S)	FONCTION
1.	SANOU Oumarou	Directeur général
2.	OUATTARA Harouna	Secrétaire général

Structure : DIRECTION GENERALE DE LA BRIGADE CENTRALE DE LUTTE CONTRE LA CYBERCRIMINALITE (BCLCC)

N° D'ORDRE	NOM ET PRENOM (S)	FONCTION
1.	YONI Bantida Samire	Cdt/BCLCC

<u>Structure</u> : DIRECTION GENERALE DE L'AGENCE NATIONALE DE SECURITE DES SYSTEMES D'INFORMATION (ANSSI)

N° D'ORDRE	NOM ET PRENOM (S)	FONCTION
1.	GANSONRE Kouka	Secrétaire général
2.	SAVADOGO Guestaba Louis Armand	DCCRE
3.	SANOGO Amidou	DEACSL
4.	CONGO Salif	DSI

SEANCE D'AUDITION DU GOUVERNEMENT DU LUNDI 1ER JUILLET 2024

LISTE DE PRESENCE DES DEPUTES

N° D'ORDRE	NOM ET PRENOM (S)	GROUPE CONSTITUE
1.	KONE Moussa	OSC
2.	TUINA Kanibè	PDCE
3.	SIDIBE Mariam	PP
4.	HIEN Diédon Alain	OSC
5.	DAMIEN/YOUL Ini Inkouraba	FVR
6.	BONZI Nonyeza	FVR
7.	KABRE Kalifa	FVR
8.	KABRE Aboubacar	PDCE
9.	ZONGO Kiswendsida Evariste	PDCE
10.	ZONGO Sayouba	PDCE
11.	NIGNAN Dida	FDS
12.	SAWADOGO Isidore Tégwendé	FDS

LISTE DE PRESENCE DES COMMISSIONS SAISIES POUR AVIS

N° D'ORDRE	NOM ET PRENOM (S)	GROUPE CONSTITUE
1.	KOMBASSERE Jean-Marie	CAGIDH
2.	TAPSOBA Issaka	COMFIB
3.	OUEDRAOGO/COMPAORE SABINE	CAEDS

LISTE DE PRESENCE DU PERSONNEL

N° D'ORDRE	NOM ET PRENOM (S)	QUALITE
1.	BAYALA Cyrille	Conseiller technique du PALT auprès de la CDD
2.	HIEN/WEDRAOGO Prisca	Administrateur parlementaire
3.	KAMBIRE B. Albert	Administrateur parlementaire
4.	OUEDRAOGO/OUEDRAOGO Aimée Edwige	Administrateur parlementaire
5.	BARRO/OUEDRAOGO Habibou W.	Secrétaire de direction
6.	OUEDRAOGO Nestor	Agent de liaison
7.	BAMOGO Jérôme	Administrateur parlementaire/CAEDS

N° D'ORDRE	NOM ET PRENOM (S)	QUALITE
8.	KYERE/YAOGO D. Téné Pascaline	Administrateur parlementaire/CAGIDH
9.	TINDANO/ZOUNDI Louise	Administrateur parlementaire/COMFIB
10.	GUIENNE Steven Amed	Agent de liaison

LISTE DE PRESENCE DES MEMBRES DU GOUVERNEMENT

N° D'ORDRE	NOM ET PRENOM (S)	FONCTION
1.	ZERBO/SABANE Aminata	Ministre
2.	YOUGBARE Boukaré	Directeur général
3.	OUATTARA/DAMA Haoua	Directrice générale
4.	SANOU Oumarou	Directeur général
5.	GANSONRE Kouka	Secrétaire général
6.	SANOGO Amidou	Directeur
7.	SAWADOGO Armand	Directeur
8.	TASSEMBEDO Abdoul Razack	Responsable département sécurité
9.	GANOU Tiébilé	DRP/MJDHRI
10.	CONGO Maïmouna	Agent GDRI

N° D'ORDRE	NOM ET PRENOM (S)	FONCTION
11.	CONGO Ibrahim Patrick	Agent SPIVETEN/MTDPCE

SEANCE D'ADOPTION DU RAPPORT DU MARDI 02 JUILLET 2024

LISTE DE PRESENCE DES DEPUTES

N° D'ORDRE	NOM ET PRENOM (S)	GROUPE CONSTITUE
1.	KONE Moussa	OSC
2.	TUINA Kanibè	PDCE
3.	SIDIBE Mariam	PP
4.	HIEN Diédon Alain	OSC
5.	DAMIEN/YOUL Ini Inkouraba	FVR
6.	BONZI Nonyeza	FVR
7.	KABRE Kalifa	FVR
8.	KABRE Aboubacar	PDCE
9.	ZONGO Kiswendsida Evariste	PDCE
10.	ZONGO Sayouba	PDCE
11.	NIGNAN Dida	FDS
12.	SAWADOGO Isidore Tégwendé	FDS

LISTE DE PRESENCE DES COMMISSIONS SAISIES POUR AVIS

N° D'ORDRE	NOM ET PRENOM (S)	GROUPE CONSTITUE
1.	KOMBASSERE Jean-Marie	CAGIDH
2.	TAPSOBA Issaka	COMFIB
3.	OUEDRAOGO/COMPAORE SABINE	CAEDS

LISTE DE PRESENCE DU PERSONNEL

N° D'ORDRE	NOM ET PRENOM (S)	QUALITE
1.	BAYALA Cyrille	Conseiller technique du PALT auprès de la CDD
2.	HIEN/WEDRAOGO Prisca	Administrateur parlementaire
3.	KAMBIRE B. Albert	Administrateur parlementaire
4.	OUEDRAOGO/OUEDRAOGO Aimée Edwige	Administrateur parlementaire
5.	BARRO/OUEDRAOGO Habibou W.	Secrétaire de direction
6.	OUEDRAOGO Nestor	Agent de liaison
7.	BAMOGO Jérôme	Administrateur parlementaire/CAEDS

N° D'ORDRE	NOM ET PRENOM (S)	QUALITE
8.	KYERE/YAOGO D. Téné Pascaline	Administrateur parlementaire/CAGIDH
9.	TINDANO/ZOUNDI Louise	Administrateur parlementaire/COMFIB
10.	GUIENNE Stevenn Amed	Agent de liaison

LISTE DE PRESENCE DES MEMBRES DU GOUVERNEMENT

N° D'ORDRE	NOM ET PRENOM (S)	FONCTION
1.	CONGO Ibrahim	Expert Juriste SPIVTEN/MTDPCE
2.	ZERBO/SABANE Aminata	Ministre
3.	YOUGBARE Boukaré	Directeur général
4.	OUATTARA/DAMA Haoua	DG/DGTD
5.	SAWADOGO Oumarou	DG/ANPTIC
6.	SANOGO Amidou	Directeur
7.	GANSONRE Kouka	SG/ANSSI
8.	SAVADOGO Armand	Directeur
9.	BATAKO A. Wilfried	Directeur /DGTD
10.	GANOU Tiébilé	DRIP/MJDHRI