PREMIÈRE SESSION EXTRAORDINAIRE DE L'ANNEE 2026

RAPPORT

FAIT AU NOM DE

L'INTERCOMMISSION CONSTITUÉE PAR LA COMMISSION DE LA CULTURE ET DE LA COMMUNICATION ET LA COMMISSION DES LOIS, DE LA DÉCENTRALISATION, DU TRAVAIL ET DES DROITS HUMAINS SUR

LE PROJET DE LOI N° 25/2026 SUR LA PROTECTION DES INFRASTRUCTURES D'INFORMATIONS CRITIQUES ET LA SÉCURITÉ NUMÉRIQUE

PAR

M.OUSMANE DIOP

RAPPORTEUR

Monsieur le Président,

Messieurs les Ministres,

Chers Collègues,

L'Intercommission constituée par la Commission de la Culture et de la Communication et la Commission des Lois, de la Décentralisation, du Travail et des Droits humains s'est réunie le jeudi 13 Août 2026, sous la présidence de Monsieur Aliou SENE, Président de la Commission de la Culture et de la Communication, à l'effet d'examiner le projet de loi n° 25/2026 sur la Protection des Infrastructures d'Informations critiques et la Sécurité numérique.

Le Gouvernement était représenté par Messieurs Samba DIOUF, Ministre des Télécommunications et du Numérique et Bacary SARR, Ministre de la Communication et des Relations avec les Institutions, Porte-parole du Gouvernement.

Ouvrant la séance, Monsieur le Président a, au nom de l'Intercommission, souhaité la bienvenue à Messieurs les Ministres, avant de donner la parole au Ministre des Télécommunications et du Numérique pour la présentation de l'exposé des motifs .

À l'entame de son propos, Monsieur le Ministre s'est réjoui de se retrouver devant la Représentation nationale, pour présenter le projet de loi portant sur la Protection des Infrastructures d'Informations critiques et la Sécurité numérique.

À cet effet, il a d'abord rappelé que le développement des Technologies de l'Information et de la Communication (TIC) a ouvert à notre pays un vaste champ d'opportunités en matière d'efficience, de compétitivité et d'inclusion.

Il a précisé que l'ensemble des activités administratives, économiques et sociales, rendues plus performantes grâce à l'usage des TIC, sont toutefois exposées, dans le même temps, aux menaces inhérentes au cyberespace, notamment le terrorisme, l'espionnage, le piratage informatique et les risques liés à la négligence humaine

À cet égard, il a indiqué que, pour se prémunir contre ces menaces, notre pays s'est doté d'un cadre juridique couvrant notamment les domaines de la confiance

numérique, du contrôle réglementaire de la cryptographie, de la protection des informations sensibles de l'État, des communications électroniques, des transactions électroniques et de la lutte contre la cybercriminalité.

Cependant, il a relevé que, malgré ces avancées, le cadre juridique existant présente encore certaines limites qu'il convient de combler afin de renforcer le niveau de sécurité numérique au Sénégal et de le hisser au niveau des meilleurs standards internationaux.

Sous ce rapport, il a fait savoir que c'est précisément pour relever ces défis que le présent projet de loi vise à mettre en place un cadre juridique global consacré à la sécurité des réseaux et des systèmes d'information utilisés pour fournir des services au Sénégal. À cet effet, il établit des principes fondamentaux de cybersécurité, tout en laissant aux autorités réglementaires le soin de préciser et de compléter ces principes, en fonction des exigences et des spécificités liées à leur mise en œuvre.

Poursuivant son propos, il a indiqué que, pour tenir compte des impératifs d'autonomie stratégique et de souveraineté, qui constituent le socle de l'Agenda national de Transformation « Sénégal 2050 », et favoriser l'émergence de champions nationaux, le présent projet de loi prévoit de confier la fourniture de certains services essentiels de cybersécurité à des prestataires agréés. Selon Monsieur le Ministre, cette initiative permettra de structurer et de développer une véritable économie de la cybersécurité autour d'acteurs de confiance, exerçant leurs activités dans un cadre défini par les lois et règlements.

Intervenant à la suite de Monsieur le Ministre, vos Commissaires lui ont d'abord réitéré leurs félicitations et encouragements, avant de lui faire part de leurs suggestions et préoccupations.

Ils ont, à l'unanimité, salué l'examen de ce projet de loi relatif à la protection des Infrastructures d'Informations critiques et à la Sécurité numérique, qu'ils ont jugé

opportun au regard de la recrudescence des cyberattaques et de la nécessité de renforcer la protection des infrastructures stratégiques du pays.

À cet égard, ils se sont interrogés sur la capacité du nouveau dispositif juridique à faire face efficacement aux attaques liées à la délinquance transfrontalière et ont souhaité être édifiés sur l'origine des principales attaques dont le Sénégal a été victime ces derniers mois, ainsi que sur les mesures prises ou envisagées par le Gouvernement pour prévenir et contenir d'éventuelles nouvelles menaces.

Dans le même sillage, vos Commissaires ont insisté sur la nécessité de doter l'Autorité nationale de cybersécurité de moyens humains, techniques et financiers suffisants. Ils ont ainsi souhaité connaître son organe de rattachement, les mécanismes de financement prévus ainsi que l'existence d'un budget spécifique consacré à la lutte contre les cyberattaques.

Ils se sont interrogés, par ailleurs, sur les critères permettant de qualifier une infrastructure de « critique » et sur l'autorité chargée de cette classification. Ils ont également souhaité connaître les mesures prévues pour assurer une évaluation régulière des risques et l'actualisation des dispositifs de protection, ainsi que les sanctions applicables en cas de non-respect des obligations de sécurité.

Relativement à la gouvernance du secteur, vos Commissaires ont attiré l'attention de Monsieur le Ministre sur la nécessité de clarifier les mécanismes de coordination entre l'Autorité nationale de Cybersécurité et l'Autorité de Régulation des Télécommunications et des Postes (ARTP) et les différents régulateurs sectoriels, afin d'éviter les chevauchements de compétences et de garantir une action publique cohérente et efficace. Ils ont également demandé des précisions sur les sanctions prévues en cas de non-respect des obligations de sécurité imposées par le projet de loi.

Dans le même ordre d'idées, ils ont souhaité être édifiés sur les dispositions transitoires à prévoir pour assurer la continuité des missions de l'Autorité nationale

de Cybersécurité. A cet égard, ils ont proposé, par voie d'amendement, de préciser que ces missions pourraient, à titre transitoire, être exercées par des structures désignées à cet effet, tout en encadrant cette période dans le temps, afin d'éviter que cette mesure provisoire ne vide la loi de sa substance.

Sur un autre registre, ils ont accordé une attention particulière à la souveraineté numérique et à la protection des données personnelles. Ils se sont interrogés sur les garanties offertes lorsque certaines données sensibles sont confiées à des entreprises étrangères, notamment dans le cadre de la confection des cartes nationales d'identité et des permis de conduire.

Vos Commissaires ont, également, souhaité savoir si le Sénégal dispose des capacités techniques et financières nécessaires pour héberger ces données sur son Territoire. Ils ont aussi demandé à connaître les critères justifiant leur stockage à l'étranger ainsi que les mesures envisagées, le cas échéant, pour leur rapatriement.

Dans la même dynamique, ils ont demandé si les données du secteur de l'éducation étaient couvertes par le dispositif et ont attiré l'attention de Monsieur le Ministre sur la situation des opérateurs de télécommunications, qui gèrent d'importants volumes de données critiques, notamment au regard de l'exclusion des réseaux de communications électroniques ouverts au public du champ d'application du projet de loi.

Vos Commissaires ont aussi insisté sur la nécessité de prendre en compte les enjeux d'inclusion et d'accessibilité. Ils ont notamment souhaité savoir si les infrastructures critiques et les services d'urgence numérique seront accessibles aux personnes vivant avec un handicap, et si celles formées aux métiers du numérique pourront intégrer le secteur de la cybersécurité. Ils ont également demandé des précisions sur les conditions d'agrément des prestataires, notamment leur caractère national ou étranger.

Concernant les nouveaux défis technologiques, ils ont souhaité connaître les mesures envisagées pour prendre en compte l'intelligence artificielle dans le champ dudit projet de loi et ont plaidé pour la mise en place de garde-fous permettant notamment de mieux protéger les enfants sur Internet.

Ils ont également demandé si une évaluation de la cohérence entre la stratégie nationale « Sénégal numérique 2025 » et la Stratégie nationale de cybersécurité a été réalisée et partagée avec les acteurs concernés. Ils ont, en outre, interrogé Monsieur le Ministre sur la capacité technique du Sénégal à mener à bien le projet d'Etat civil.

Sur un autre plan, ils l/ont interpellé sur le retard accusé dans la prise du décret d'application relatif à l'indemnité spéciale de discrétion professionnelle des agents de la Direction du Chiffre et de la Sécurité des Systèmes d'Information, prévue depuis 2014. Ils ont considéré cette situation comme une injustice qu'il convenait de corriger.

Enfin, sur la forme, vos Commissaires ont relevé certaines incohérences et insuffisances rédactionnelles dans le projet de loi. Ils ont notamment signalé que quatre chapitres sont annoncés alors que le texte en comporte cinq. Ils ont également relevé l'absence de définition de certaines notions essentielles, estimant que leur clarification est nécessaire pour garantir une meilleure compréhension et une application uniforme du dispositif.

Ils ont, en définitive, estimé que l'efficacité de cette réforme dépendra de la clarté du cadre juridique, mais également des moyens financiers, techniques et humains mobilisés, de la coordination des acteurs et de la capacité du Sénégal à garantir sa souveraineté numérique. Ils ont ainsi, invité Monsieur le Ministre à apporter les clarifications nécessaires sur ces différents points afin de garantir une mise en œuvre effective et durable de la politique nationale de cybersécurité.

Reprenant la parole, Monsieur le Ministre a salué le bon déroulement des débats ainsi que la pertinence des différentes problématiques abordées. Il a également

apprécié ce moment fort d'échanges, d'expression et d'accompagnement de la part des commissaires, qu'il a chaleureusement remerciés pour leurs prières et leurs encouragements.

D'emblée, il a salué la diversité des sensibilités exprimées. Selon lui, le projet de loi portant protection des Infrastructures d'Informations critiques et la Sécurité numérique s'inscrit dans la sécurisation et la défense de nos systèmes d'information et plateformes numériques, qui touche à des principes essentiels, la souveraineté numérique et la responsabilité des gestionnaires d'infrastructures d'information critique.

Concernant la définition de certains termes techniques, Monsieur le Ministre a précisé que Le CERT est une équipe chargée d'alerter sur les menaces et prévenir les risques sur les systèmes d'information, de réagir en cas d'incident de sécurité informatique et d'aider à atténuer les effets. Ainsi, dans le jargon de cybersécurité, existe des termes qui définissent comment doit être organisé le dispositif de cyber pour répondre aux différentes attaques.

Au sujet de l'inclusion d'office des infrastructures d'informations critiques, il a précisé qu'il s'agit d'infrastructures présentant des caractéristiques particulières et nécessitant, à ce titre, un traitement spécifique. S'agissant des institutions de la République comme l'Assemblée nationale, une procédure d'identification et de classification sera mise en œuvre. Il a indiqué que la liste des infrastructures ainsi identifiées sera tenue secrète et ne figurera pas dans le texte de loi.

À cet égard, il a rassuré les Commissaires quant à la mise en place d'une classification des infrastructures d'informations critiques, laquelle sera protégée au titre du secret de la défense nationale.

Par ailleurs, concernant l'assurance contre les risques de cybersécurité, il a rappelé qu'elle demeure, de manière générale, une option pour les structures. Toutefois, le projet de loi donne aux autorités compétentes la possibilité de la rendre obligatoire

dans certains secteurs ou pour certains acteurs particulièrement exposés aux cyberattaques, notamment lorsque le risque de dommages importants est élevé. Ainsi, d'après lui, si une certaine flexibilité est laissée aux structures quant à leur adhésion à cette assurance, la loi permet également aux autorités d'en imposer la souscription à certaines catégories d'acteurs jugées particulièrement vulnérables.

S'agissant des menaces transfrontalières, il a rassuré vos Commissaires quant aux dispositifs de sécurité et de riposte mis en place pour faire face à ces menaces multiformes. Il a également assuré que ces dispositifs seront renforcés afin de mieux prendre en compte l'évolution et la diversité de ces menaces.

À propos de la provenance des cyberattaques, il a indiqué qu'elles provenaient principalement d'Europe, d'Asie et même d'Afrique. Elles sont particulièrement motivées par des considérations financières, notamment dans le cadre d'attaques par rançongiciel, au cours desquelles une rançon est demandée en échange de la restitution des données ou de la non-publication de celles-ci.

Pour ce qui concerne le traitement salarial du personnel du Chiffre, Monsieur le Ministre a relevé que cette question n'était pas de son ressort mais de celui du Ministre, Secrétaire général de la Présidence de la République. Il a cependant relevé que les informations qui lui avaient été communiquées établissaient que la loi de 1983 régissant le statut du personnel du Chiffre, modifiée en 1974, avait déjà des décrets d'application. En tout état de cause, Monsieur le Ministre a affirmé qu'il avait pris bonne note de la préoccupation soulevée, et a indiqué qu'il va saisir les autorités compétentes des préoccupations exprimées par les députés.

Concernant la place de l'Etat dans la gestion de la SONATEL, il a indiqué qu'il s'agit d'une société privée dont l'État détient 27 % (vingt-sept pour cent) du capital. La société étant cotée en bourse, cela justifie l'absence d'ingérence de l'État dans son fonctionnement courant. En revanche, l'État intervient particulièrement dans la gouvernance de cette société à travers son Conseil d'Administration. Ainsi, aucune

décision majeure n'est prise au sein de cet organe sans l'accord et l'approbation de l'État du Sénégal, a-t-il ajouté.

Relativement à la demande de précision sur l'ancrage des missions de l'Autorité nationale de Cybersécurité, il a précisé que cette autorité est actuellement rattachée à la Présidence de la République. Son ancrage institutionnel et son fonctionnement seront déterminés par décret, conformément aux orientations de Monsieur le Président de la République.

Pour les critères et identification permettant de classer une infrastructure d'information critique et les sanctions prévues en cas de manquement, il a expliqué que les articles 21, 22 et 23 du présent projet de loi, les prennent en compte et les éventuelles sanctions sont également prévues dans le chapitre 4 du projet de loi.

Sur l'existence d'un cadre permettant de coordonner les activités de l'autorité de la cybersécurité, l'ARTP et les autres régulateurs sectoriels, il a précisé qu'un projet de cadre de co-régulation entre l'ARTP et la Commission de Protection des Données Personnelles (CDP), est en cours et permettra une meilleure coordination entre les différents acteurs intervenant dans le secteur de la régulation.

Concernant le paiement de rançons à la suite des multiples cyberattaques dont le Sénégal a récemment été victime, il a souligné qu'à sa connaissance, une telle situation ne s'était jamais produite au Sénégal. Il a également indiqué que notre pays dispose de moyens de défense et de capacités nécessaires pour riposter efficacement aux attaques de cybersécurité. Sur l'évaluation de la Stratégie nationale SN2025, il a confirmé que celle-ci avait déjà été réalisée.

Relativement à la question de savoir si le Sénégal dispose de capacités techniques pour stocker l'ensemble de nos données, répondant par l'affirmatif, il a aussi indiqué que le stockage des données sur le Territoire national sera assuré à la fois par des infrastructures publiques appartenant à l'État et par des prestataires privés agréés. L'Autorité nationale de Cybersécurité définira les référentiels permettant

d'homologuer ces prestataires privés offrant des services de cloud sur le sol sénégalais.

Sur le dispositif pour autoriser le stockage de données à l'étranger, il a souligné que concernant les données de l'État, le principe est qu'elles doivent être conservées sur le Territoire national. Toutefois, en raison de la dépendance technologique du pays, des exceptions sont prévues pour autoriser à titre exceptionnel l'hébergement ou le traitement de ces données à l'étranger.

Pour les autres catégories de données, il a rappelé que les règles d'hébergement et de traitement seront fixées par décret, une approche réglementaire et modulaire jugée plus adaptée à la complexité du sujet. A ce titre, il a précisé que l'Autorité nationale de Cybersécurité est chargée d'établir le référentiel de sécurisation correspondant.

Réagissant à l'intervention relative à la capacité de notre pays à mener à bien le projet de modernisation de l'Etat civil, il a indiqué que l'Agence nationale de l'État civil (ANEC) joue pleinement son rôle sur l'ensemble du Territoire national, à travers plusieurs activités de sensibilisation et de vulgarisation visant à assurer la réussite de ce projet, particulièrement important pour le Sénégal. Il a également précisé que les données issues de ce projet seront sauvegardées au niveau du Data Center de Sénégal Numérique (SENUM).

Sur l'accessibilité des sites aux personnes vivant avec un handicap et leur intégration dans le secteur de la cybersécurité pour celles formées aux métiers du numérique, il a souligné que cette préoccupation est particulièrement prise en compte dans la construction des infrastructures, afin de faciliter l'accès à cette catégorie de personnes. Il a également précisé que la loi ne fait aucune discrimination à leur égard et qu'elles pourront pleinement exercer leurs compétences et travailler au sein de ces infrastructures.

Concernant le dispositif des prestataires agréés et la participation des acteurs étrangers, Monsieur le Ministre a rappelé que les prestataires agréés sont prévus par

l'article 15 du projet de loi et l'objectif est d'organiser l'écosystème cyber qui permet de protéger les infrastructures critiques, créer des champions nationaux, et ouvrir le marché à la cybersécurité.

Abordant l'interpellation relative à l'exclusion des réseaux de télécommunications électroniques du champ des infrastructures critiques, il a indiqué que ceux-ci constituent une composante essentielle de l'écosystème numérique et qu'ils ne sont, par conséquent, pas exclus du champ d'application dudit projet de loi.

Sur la question de l'organe chargé de veiller à la sécurité numérique du pays, il a indiqué que la Direction générale du Chiffre et des Sécurités des Systèmes d'Information est chargée de la mise en œuvre de la politique de sécurité et de défense des systèmes d'information, définie par Monsieur le Président de la République, en vue de promouvoir au Sénégal un environnement numérique de confiance, sécurisé et résilient.

Poursuivant, il a expliqué que pour la protection des enfants en ligne, le ministère du Numérique met en œuvre le plan d'action de protection des enfants en ligne, PAPEL, et travaille en étroite collaboration avec le ministère en charge de la Famille et la Cellule d'Appui de la Protection des enfants. Il se rapprochera de son homologue Monsieur le Ministre de la Communication notamment avec le Conseil de régulation des médias pour les contenus audio -visuels.

De même, pour la prise en compte des infrastructures critiques situées en zone rurale, il a précisé qu/elles sont toutes sont concernées par la présente loi, quel que soit leur emplacement sur le Territoire national.

Pour ce qui concerne la prise en charge de l'Intelligence artificielle dans le cadre du projet de loi, Monsieur le Ministre a précisé qu/ à l'instar de l'ensemble des technologies émergentes, elle est prise en compte dans ledit projet.

Toutefois, il a indiqué qu'il n'était pas opportun de citer spécifiquement cette technologie dans le texte législatif, compte tenu de son caractère évolutif. C'est pourquoi le projet de loi s'attache à consacrer le principe général de cybersécurité. Il a, en outre, ajouté que des référentiels et des normes techniques permettront d'assurer la prise en compte détaillée de ces technologies, notamment l'Intelligence artificielle.

Au sujet de l'introduction d'une disposition transitoire visant à encadrer, dans le temps, l'exercice des missions de l'Autorité nationale de Cybersécurité qui pourraient être assurées par d'autres structures, il a indiqué que son département propose d'engager une concertation avec l'Assemblée nationale à l'issue de la réunion, en vue de discuter d'un amendement au dernier alinéa de l'article 6, lequel pourrait être proposé lors de l'examen du texte en séance plénière.

En somme, s'agissant des préoccupations de forme soulevées, il a assuré avoir pris bonne note des remarques formulées et s'est déclaré favorable aux modifications proposées, sous réserve d'amendements à examiner en concertation avec les membres de la Commission

Satisfaits des réponses apportées par Monsieur le Ministre, vos Commissaires ont adopté, à l'unanimité le projet de loi n° 25/2026 portant sur la Protection des Infrastructures d'Informations critiques et la Sécurité numérique. Ils vous demandent d'en faire autant, si cela ne soulève, de votre part, aucune objection majeure.