

3^e Edition
Forum
**SUR LA GOUVERNANCE
DE L'INTERNET AU MALI**
Juillet 2025



Sommaire

Introduction.....	2
Processus de proposition des thématiques	4
Ouverture des travaux	6
Deroulement des travaux	8
Panel 1 : Gouvernance de l'Internet; défis et perspectives pour un Internet ouvert accessible et résilient au MALI ?.....	8
Panel 2 : Souveraineté numérique face aux technologies disruptives : quelles stratégies pour les États ?.....	12
Panel 3 : Cyber sécurité et résilience des infrastructures critiques à l'ère des ruptures technologiques.....	15
Panel 4 : Données personnelles et vie privée à l'ère des technologies émergentes : quels enjeux pour la jeunesse et l'égalité de genre ?.....	18
Panel 5 : L'IA au service de l'innovation technologique et de l'entrepreneuriat numérique : défis, enjeux et perspectives.....	21
Recommandation.....	24
Annexe.....	28
Données démographiques.....	28
Liste des Intervenants.....	33
Agenda du forum.....	35
Equipe de redaction.....	37



I. Introduction

Le Mali traverse une période de crises multidimensionnelles (sécuritaire, politique et socio-économique) qui impactent profondément son développement et exigent des solutions innovantes. Dans ce contexte, les technologies de rupture notamment l'Intelligence Artificielle (IA), la Blockchain, la 5G, l'Internet des Objets (IoT) représentent à la fois une opportunité de résilience et un défi énorme de gouvernance.

Pourtant, le Mali ne dispose pas encore d'un cadre réglementaire adapté pour ces technologies dites disruptives. Cette absence de régulation pose comporte des risques majeurs en termes de leurs usages particulièrement dans le domaine de la cybersécurité et l'utilisation des données dans l'IA ; l'éthique et la transparence des algorithmes ; la souveraineté numérique.

Le Forum sur la Gouvernance de l'Internet au Mali (FGI-Mali), plateforme essentielle de dialogue multipartite par excellence, est resté en veille depuis 2021 malgré l'urgence des enjeux de l'avenir du numérique au Mali. Face à l'accélération des disruptions technologiques, il s'est avéré impératif de redynamiser cette plateforme pour aborder des questions telles que l'Intelligence Artificielle qui nous frappe de plein fouet ; la souveraineté (numérique) qui est devenue la boussole de navigation de notre nation ; la gouvernance des infrastructures et la cybersécurité etc.

Cette 3^{ème} édition s'est fixé comme mission de mobiliser tous les acteurs, Gouvernement, Secteur privé, Société civile, Chercheurs... autour d'une question centrale : Comment le Mali peut-il tirer profit des technologies de rupture tout en garantissant un Internet stable, ouvert et au service du développement.

C'est ainsi que, l'évènement a été placé sous le thème central : « Technologies de ruptures face aux perspectives de la Gouvernance de l'Internet » ; un thème qui va explorer les tensions entre les innovations disruptives et les mécanismes de régulation du numérique. Il est aujourd'hui incontestable que les bouleversements induits par les technologies de rupture. Leur rapidité d'évolution et leur caractère décentralisé remettent en question les cadres juridiques et éthiques existants, nécessitant une adaptation urgente et constante des systèmes de gouvernance pour éviter des dérives tout en favorisant l'innovation.

Ce débat soulève une question fondamentale : comment concilier innovation et contrôle démocratique? D'un côté, une régulation trop stricte risquerait de brider le progrès technologique ; de l'autre, un laisser-faire exposerait les sociétés à des risques majeurs (cybercriminalité, surveillance de masse, augmentation des inégalités). L'avenir de la gouvernance d'Internet dépendra donc de la capacité à inventer des modèles hybrides, associant éthique, coopération internationale et flexibilité, pour encadrer les bonds technologiques sans les étouffer.

Ainsi pour mieux discuter des différents aspects de cette thématique, la 3e édition de FGI MALI a été déclinée en cinq sous-thèmes qui ont été discutés en panel et deux keynotes de cadrage. Les différents sous-thèmes qui ont fait l'objet de discussions et rapportés sont les suivants :

Panel 1 : Gouvernance de l'Internet : défis et perspectives pour un Internet ouvert accessible et résilient au Mali.

Panel 2 : (panel de haut niveau) : Souveraineté numérique face aux technologies disruptives : quelles stratégies pour les États ?

Panel 3 : Cybersécurité et résilience des infrastructures critiques à l'ère des ruptures technologiques.

Panel 4 : Données personnelles et vie privée à l'ère des technologies émergentes : quels enjeux pour la jeunesse et l'égalité de genre ?

Panel 5 : L'IA au service de l'innovation technologique et de l'entrepreneuriat numérique : défis, enjeux et perspectives.

KeyNote 1 : Gouvernance de l'Internet face aux technologies émergentes : quel équilibre entre Régulation et Innovation.

KeyNote 2 : L'IA et la Cybersécurité : nouveaux pouvoirs, nouvelles responsabilités pour la Gouvernance de l'Internet.



II. Processus de proposition des thématiques

L'inclusivité au sens large du terme est un des piliers importants du Forum sur la gouvernance de l'Internet. Cette inclusivité doit marquer toutes les étapes du forum. Depuis le choix des thématiques jusqu'au choix des intervenants. L'ensemble des parties prenantes doit se retrouver dans les thématiques et même parmi les intervenants.

À cet effet la troisième édition du Forum sur la Gouvernance de l'Internet au Mali n'a pas dérogé à cette règle. En ce qui concerne la proposition des thématiques, le thème central a été défini par le MAG dans lequel les parties prenantes sont représentées comme suit : 2 membres du Gouvernement, 2 du secteur privé, 2 de la société civile et 1 de l'université. Après avoir arrêté le thème « **Technologies de rupture face aux perspectives de la Gouvernance de l'Internet** » comme thème central, il a été question de définir les sous-thèmes devant faire l'objet de discussion dans les panels.

Dans un premier temps, un appel à proposition de thèmes a été lancé sur le site www.fgimali.ml afin de recueillir les propositions des différentes parties dans le souci de prendre en compte les préoccupations de tous. A la suite de cet appel, 11 thèmes ont été reçus. Il faut signaler que la 3e édition du Forum dans son agenda initial devait se tenir en 2 jours avec 8 panels prévus.

Compte tenu des difficultés budgétaires dues à la situation globale du Mali elle-même, les organisateurs ont été obligés de revoir leurs ambitions à la baisse.

Ainsi le forum a été réduit à un seul jour avec 5 panels et 2 keynotes.

Une fois l'appel à proposition bouclé, le MAG et certains volontaires ayant de l'expérience sur la question ont passé en revue les 11 thèmes et en ont fusionné certains afin de nous proposer les 5 thèmes qui ont été retenus. Vu la pertinence de certains thèmes n'ayant pas été retenus lors des discussions, ils ont été reformulés pour les Keynotes.

Une fois les thèmes arrêtés, nous sommes passés au choix des intervenants (panelistes et modérateurs). A ce stade aussi nous avons tenu compte de toutes les sensibilités. Il est à souligner que compte tenu des disponibilités des uns et des autres pour la date arrêtée, nous n'avons pas pu respecter les quotas comme on avait prévu c'est-à-dire avoir toutes les parties prenantes et avec un équilibre de genre.

Parmi les intervenants, on pouvait noter ceux venant de l'administration publique, du secteur privé, de l'armée, de la société civile (voir la liste des intervenants en annexe).

Nous signalons que cette 3e édition du forum du Mali a été entièrement financé par la fondation Internet Society à travers le chapitre malien de l'Internet Society.



III. Ouverture des travaux du Forum



La cérémonie d'ouverture a été très riche en couleurs. Elle a enregistré la présence d'éminentes personnalités du secteur à commencer par le Ministre de la Communication, de l'Economie Numérique et de la Modernisation de l'Administration M. Alhamdou Ag ILYENE et de son cabinet. D'autres anciens ministres et des anciens secrétaires généraux du Ministère en charge des TIC étaient également présents.

Nous avons noté la présence du Président de l'Autorité de Protection des Données à Caractère Personnel, du Directeur général de l'Agence des Technologies de l'Information et de la Communication, du Directeur Général de l'Agence Nationale de Télésanté et d'Informatique Médicale, du Directeur Général de Atribone Mali, de la Directrice du Service de Certification et de Signature Electronique, de la Direction Nationale de l'Economie Numérique, des membres de ML CERT et plusieurs autres personnalités.

Dans une salle pleine à craquer, la cérémonie d'ouverture a commencé par une présentation faite par le doyen Dr Mamadou Diallo lam (Président du Groupe des experts lors du SMSI à Genève en 2003). Le Dr Diallo a brossé l'historique du forum en mettant en exergue le rôle crucial que le Mali a joué à l'époque. Il a terminé sa présentation par le souhait d'un FGI-MALI dynamique et inclusif.

Le second intervenant fut le Président de FGI-MALI en la personne de M Bakary KOUYATE. Il a placé son discours sous le signe d'un nouveau départ qui marquera un tournant décisif dans la gouvernance de l'internet au Mali.

Il a rappelé la disruption technologique et les défis de cette ère tout en demandant aux décideurs qu'une attention soit portée aux recommandations des travaux. Il a terminé son discours par un plaidoyer en faveur du FGI pour un soutien institutionnel et financier renforcé.

La troisième intervention fut celle de M. Emmanuel Elogo Agbenonwossi, Coordonnateur du Secrétariat du Forum Ouest Africain sur la Gouvernance de l'Internet (WAIGF). M. Agbenonwossi a rappelé le rôle précurseur joué par le Mali dans l'instauration de la gouvernance du numérique en Afrique. Il a centré son intervention sur l'actualité du thème choisi, la problématique des technologies de rupture étant discutée au sein du WAIGF depuis 2024. Ainsi, le Mali s'inscrit pleinement dans la continuité de ces réflexions.

M. Agbenonwossi a réitéré le soutien du secrétariat du WAIGF au Forum du Mali pour sa structuration durable.

Pour conclure, il a encouragé les autorités maliennes ainsi que l'ensemble de l'écosystème à s'engager dans les discussions internationales actuelles, notamment dans le cadre de l'examen des 20 ans du SMSI, de l'élaboration du pacte numérique mondial et des débats sur l'avenir de la gouvernance mondiale de l'Internet.

Le discours d'ouverture a été prononcé par M. Alhamdou Ag ILYENE, Ministre de la Communication, de l'Économie Numérique et de la Modernisation de l'Administration du Mali.

Monsieur le Ministre a introduit son discours en situant la 3^e édition du forum dans son contexte. Il a rappelé que cette plateforme multipartite sert de cadre pour analyser l'impact des technologies émergentes (IA, Blockchain, 5G, IoT) sur le développement socio-économique du Mali. Il a identifié les défis prioritaires à relever que sont la cybersécurité, la protection des données, la régulation de l'IA, l'éthique des algorithmes, la souveraineté et la citoyenneté numérique.

Il a affirmé que le FGI-Mali constitue une opportunité pour se pencher sur ces défis dans le contexte malien et africain, afin d'appréhender les problèmes et d'anticiper les solutions possibles, ce qui permettra de réduire leurs impacts négatifs sur notre économie et notre société.

Pour conclure, M. le Ministre a réaffirmé le soutien de son département à cette initiative et son engagement à examiner les recommandations issues des discussions en faveur d'une gouvernance inclusive d'un Internet plus résilient.



IV. Déroulement

Ce document mettra en lumière les points essentiels soulevés lors des débats et un résumé des discussions panel par panel. Il conclura sur les recommandations formulées lors des différents panels.



Panel 1 : Gouvernance de l'Internet : défis et perspectives pour un Internet ouvert accessible et résilient au MALI ?

1.1. Points soulevés

Au cours de ce débat, les principaux points suivants ont été soulevés.

L'inclusivité d'une gouvernance participative de l'Internet

La gouvernance de l'Internet ne peut être efficace que si elle repose sur une approche inclusive, consensuelle et partagée. Elle doit impliquer tous les acteurs concernés (pouvoirs publics, secteur privé, société civile, communauté technique et le monde académique) dans la définition des règles et décisions guidant le développement du numérique. L'objectif est de construire, avec et pour l'ensemble des acteurs, un écosystème numérique harmonieux, éthique et durable.

La persistance des défis structurels à relever

Le panel a mis en exergue les nombreux obstacles auxquels le Mali est confronté. Bien que le retard numérique en soi puisse représenter une opportunité pour construire de façon solide, plusieurs autres défis restent critiques : absence de lois adaptées, manque de compétences locales, infrastructures insuffisantes, faible formation des utilisateurs, manque de sensibilisation à grande échelle...

L'inégalité d'accès à Internet

Le panel a alerté sur les profondes inégalités d'accès à Internet au Mali. Le coût élevé des services, l'insuffisance des infrastructures particulièrement dans les zones rurales, et le manque de contenus adaptés rendent l'Internet peu accessible. À cela s'ajoute un analphabétisme numérique préoccupant qui accentue la fracture entre les différentes couches sociales.

La résilience du réseau comme enjeu stratégique

La résilience de l'infrastructure Internet doit être une priorité nationale. Il s'agit de la capacité des systèmes informatiques à résister aux perturbations qu'elles soient naturelles techniques ou humaines et à se rétablir efficacement. Cela exige des infrastructures diversifiées avec des redondances, une coopération entre les acteurs pour une sécurité renforcée, mais aussi une adaptation continue aux spécificités locales et un respect des principes éthiques.

Le rôle crucial de la société civile

Dans l'écosystème du numérique, la société civile joue un rôle essentiel. Constituée d'utilisateurs, elle est la cible de tous les problèmes de cybercriminalité (arnaques, harcèlements, etc.). Elle est mieux placée pour dénoncer les dysfonctionnements de l'Internet, la mauvaise qualité, le coût d'accès élevé, bref tout ce qui peut constituer un obstacle à l'Internet ouvert. Ces préoccupations doivent être prises en compte pour renforcer la stratégie nationale dans la protection des usagers.

Une inclusion numérique plus équitable

Dans notre société, des couches socioprofessionnelles telles que les femmes, les personnes âgées, les handicapés ne sont pas assez visibles dans l'écosystème Internet. L'inclusion numérique passe par une approche globale et proactive. Quant à la population rurale, la priorité est de résoudre la problématique énergétique. Il est donc indispensable de miser sur les énergies renouvelables pour desservir les régions isolées. La formation au numérique des enfants dès leur plus jeune âge, l'organisation régulière d'événements de sensibilisation font partie des mesures indispensables à mettre en œuvre. Adopter des politiques publiques prenant en compte les besoins des populations vulnérables est une nécessité.

Anticiper l'avenir numérique du Mali

Le panel a plaidé pour une véritable vision stratégique, accompagnée de réalisations concrètes. Il a insisté sur la nécessité de favoriser les investissements dans le numérique, de bâtir des infrastructures robustes et résilientes, de mettre en place un cadre juridique favorable à l'innovation et de valoriser les solutions et contenus locaux. Le développement numérique du Mali doit s'appuyer sur ses propres talents et réalités culturelles.

L'équilibre entre liberté, sécurité et régulation

Le maintien de l'équilibre entre la liberté d'expression en ligne, la sécurité numérique et une régulation appropriée est très délicat. Il faudrait une régulation progressive, fondée sur la formation et la sensibilisation, l'information et le dialogue entre tous les acteurs pour garantir un espace numérique libre, sûr et souverain.

1.2. Résumé des discussions

La Gouvernance de l'Internet repose sur une gestion collective, inclusive et consensuelle de son évolution et de son écosystème. Elle implique la participation active de tous les acteurs (public, privé et société civile) dans l'élaboration des règles et décisions qui régissent le développement et l'utilisation de l'Internet, avec pour but une évolution harmonieuse et responsable. La société civile a un rôle fondamental à jouer, notamment en matière de cybersécurité. Elle peut proposer des solutions adaptées au contexte malien et contribuer à renforcer la stratégie nationale.

Cependant, le Mali fait face à de nombreux défis. Si le retard technologique peut être perçu comme une opportunité pour poser des bases solides, il n'en reste pas moins que les obstacles sont bien réels : inadéquation des lois, manque de ressources humaines qualifiées, manque de ressources financières, déficit de formation, et une sensibilisation encore trop faible de la population. La difficulté de l'équilibre délicat entre liberté, régulation et sécurité en ligne reste posée.

Le panel a prôné une régulation progressive, fondée sur la sensibilisation, la formation, le dialogue et la co-construction entre institutions, population et société civile. La liberté numérique doit être protégée, sans pour autant négliger les impératifs de sécurité et de souveraineté.

Cependant, l'arbre ne doit pas cacher la forêt. Il faut reconnaître une problématique cruciale : l'accès à Internet reste difficile pour une grande partie des Maliens. Les infrastructures sont peu développées, surtout dans les zones reculées, et le coût de la connexion est prohibitif. De plus, l'insuffisance de contenus numériques locaux, pertinents et attractifs, aggrave la fracture numérique, déjà alimentée par un fort taux d'analphabétisme numérique.

L'adoption de politiques publiques favorisant les groupes vulnérables est une nécessité. Le développement des énergies renouvelables, la formation dès le plus jeune âge, la multiplication des événements de sensibilisation sont autant de leviers pour améliorer l'inclusion numérique.

Par ailleurs, l'un des enjeux majeurs de la Gouvernance de l'Internet reste la résilience de l'infrastructure Internet. La résilience est la capacité des infrastructures à faire face aux chocs (qu'ils soient d'origine humaine, technique ou naturelle) et à se rétablir rapidement. Cela nécessite une diversification desdites infrastructures, un environnement technologique solide et redondant, mais aussi une collaboration sincère entre les acteurs du secteur.

La sécurité, l'éthique et l'adaptation aux réalités locales sont également au cœur de la résilience. Quant à la préparation de l'avenir numérique du Mali, le forum a insisté sur la nécessité d'une vision claire et de réalisations concrètes. Cela passe par des investissements judicieux, un cadre juridique favorable, une stratégie de contenus locaux et une valorisation des solutions innovantes issues du pays.





Panel 2 : Souveraineté numérique face aux technologies disruptives : quelles stratégies pour les États ?

2.1. Points soulevés

Au cours de ce débat, les principaux points suivants ont été soulevés.

🕒 Une vision stratégique nécessaire

Tous les panélistes s'accordent sur le fait que la souveraineté numérique ne peut être atteinte sans une vision stratégique à long terme. Elle repose sur plusieurs piliers comme les infrastructures numériques souveraines, la maîtrise des contenus (locaux), la formation des ressources humaines qualifiées, un financement continu et adapté et la protection des données nationales.

🕒 Le ccTLD .ml, symbole de souveraineté

L'extension ".ml" a été évoquée comme un symbole potentiel de souveraineté numérique, mais son efficacité dépend de son contrôle national effectif. Le rapatriement du .ml fait partie des éléments d'appréciation de notre souveraineté numérique. Le forum a salué la finalisation complète de ce processus qui n'avait que trop duré. De nos jours, le .ml est hébergé au Mali et géré par des maliens.

La maîtrise des données, comme élément de souveraineté numérique

Il n'est point possible d'être souverain sur le plan numérique avec ses données hébergées ailleurs. C'est pourquoi l'idée de créer des centres de données locaux selon les dernières normes en vigueur a été soutenue. Cela permettra d'héberger nos données en local en toute sécurité. Pour une meilleure appropriation de ce service, le coût d'hébergement dans ces centres de données doit être à la portée de l'utilisateur lambda. Pour relever ces défis, la question énergétique a été soulevée comme une nécessité urgente.

L'application sectorielle du numérique est un gage de souveraineté

Les discussions ont mis en évidence un décalage entre les besoins du pays et les moyens actuellement disponibles. La souveraineté numérique ne pourra se concrétiser que si l'État évalue l'importance multisectorielle des TIC, notamment dans l'économie, l'éducation, la santé l'agriculture et la sécurité.

La confiance numérique, un élément de taille pour une souveraineté garantie

Une réflexion a été engagée sur l'importance d'une gouvernance numérique nationale forte, portée par une volonté politique et soutenue par des solutions locales. Le développement des services en ligne, l'e-commerce, les transactions électroniques ont pour socle la confiance numérique.

Cette confiance doit être bâtie sur des supports comme la signature et la certification numérique assurée par nos propres structures. Pour l'opérationnalisation de ces structures l'État doit créer de toute urgence des infrastructures à clés publique (PKI). Une conviction partagée est que sans des plateformes nationales de confiance, il sera difficile de lutter contre la dépendance technologique et de bâtir une véritable économie numérique souveraine.

2.2. Résumé des exposés :

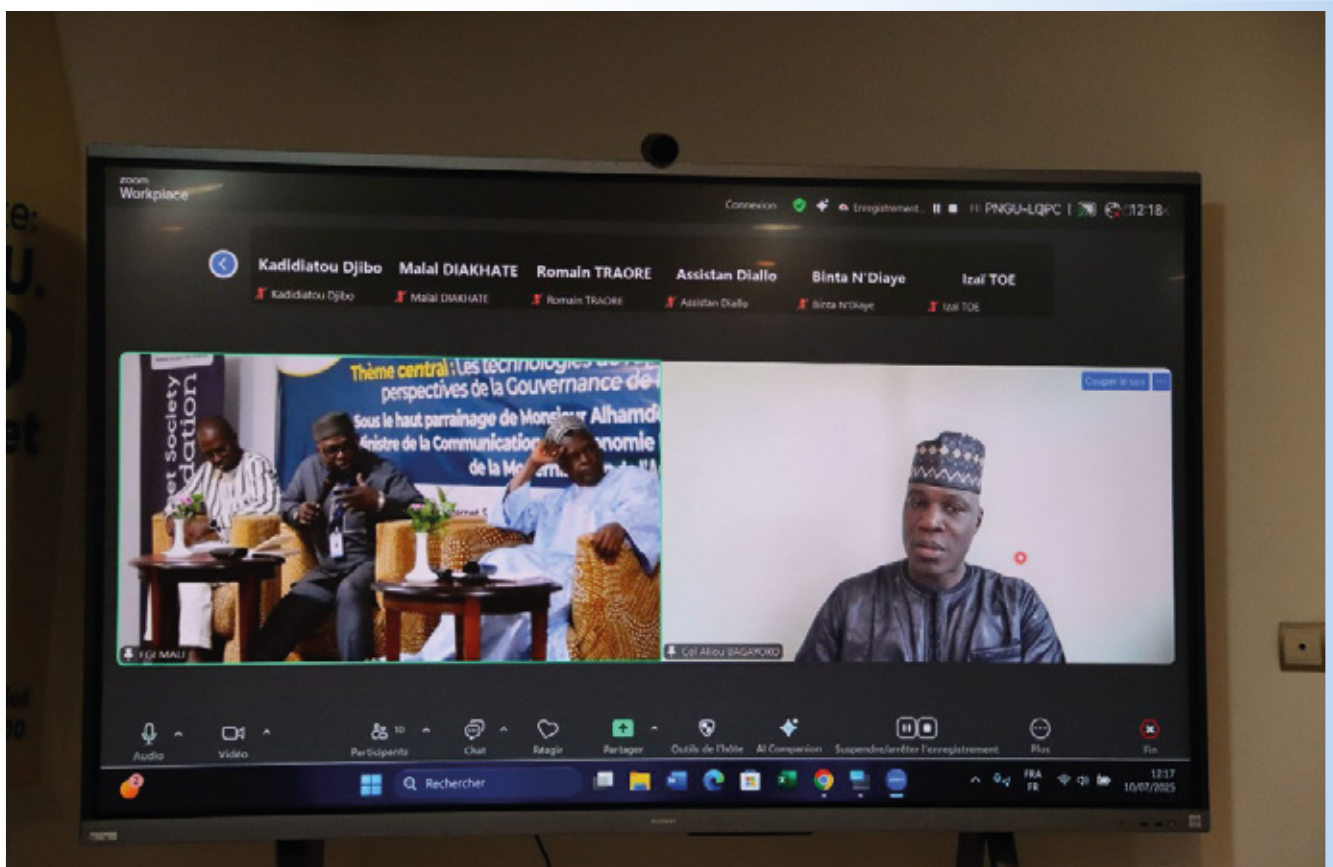
Le rôle crucial de l'Autorité Malienne de Régulation des Télécommunications, des TIC/Postes (AMRTP) dans le processus de la souveraineté a fait l'objet de discussions. Il a été clarifié que l'Autorité n'est pas responsable de l'infrastructure mais de la régulation, avec un accent sur les enjeux de sécurité dans le cyberspace.

De nos jours, le Mali n'est pas encore suffisamment outillé technologiquement, mais il est urgent d'adopter une vision claire de cybersouveraineté, centrée sur la création de centre de données nationaux où les données maliennes seront hébergées localement.

La souveraineté numérique passe également par la création de contenus adaptés aux réalités locales et par la valorisation du ccTLD malien c'est-à-dire l'extension « .ml » à partir du moment où sa gestion est effectivement localisée au Mali.

Le panel a souligné les éléments essentiels de la souveraineté numérique notamment : la formation de masse, la création d'écoles spécialisées, le recyclage des ingénieurs, et surtout la mise en place d'infrastructures robustes. Il a insisté sur la nécessité de financements continus pour soutenir la recherche, la formation et le développement de solutions locales, en encourageant particulièrement les entreprises TIC. Il est à noter que l'archivage technologique, à travers la création de plateformes de gestion, de mémoires électroniques et de serveurs dédiés, est un aspect indispensable de la souveraineté numérique. La rapidité de la mutation numérique a été mise en exergue avec des exemples comme le remplacement du Fax, du Téléx, et des cartes postales etc. Celles-ci constituent des exemples de technologies disruptives.

Le panel a rappelé les fonctions régaliennes de l'État en matière de souveraineté. L'État doit impérativement s'appropriier les technologies et les intégrer dans tous les secteurs, notamment par l'éducation, la formation et l'innovation locale. La nécessité de créer un environnement numérique souverain, en mettant en place une armée numérique intégrée, structurée autour de réseaux locaux et autonomes est impérative pour la sécurité. Il est à noter que cela peut constituer un aspect très important dans la lutte contre le terrorisme au Mali.





Panel 3 : Cyber sécurité et résilience des infrastructures critiques à l'ère des ruptures technologiques

3.1. Principaux points soulevés :

Au cours de ce débat, les principaux points suivants ont été soulevés.

La stratégie nationale de cybersécurité

L'État joue un rôle crucial dans le domaine de la cybersécurité et de la protection des infrastructures critiques. À travers sa stratégie nationale, l'État doit définir une vision claire avec des objectifs précis concernant l'évolution et à la sécurité du cyberspace malien. La mise en place de structures spécialisées pour la sécurité du cyberspace est une nécessité. Il est impératif d'envisager également le déploiement d'outils d'intelligence artificielle afin d'accélérer la mise en œuvre de plans d'actions notamment pour intégrer la cybersécurité dans le système éducatif.

Les cyberattaques, une préoccupation quotidienne

Le panel a mis en évidence à travers plusieurs exemples de cyberattaques. Cependant, des systèmes et dispositifs de protection ont été développés afin de réduire les risques et limiter l'impact de ces attaques sur certaines structures locales. Ainsi les cybermenaces sont une réalité quotidienne que vivent les structures. De nos jours nous assistons également à une mutation du terrorisme traditionnel vers le cyberterrorisme. La situation pourrait devenir extrêmement complexe en l'absence de dispositions adéquates pour faire face à ces attaques.

La prévention contre les cyberattaques

Le monde étant de plus en plus digital, nous devons prendre des mesures préventives face aux cyberattaques, qui sont souvent très rapides et inattendues et qui frappent de nombreuses organisations et individus. À cet effet, nous devons mettre en œuvre des solutions de cyberprotection efficaces ; disposer d'outils performants pour surveiller et sécuriser les systèmes ; analyser quotidiennement les systèmes sensibles ; identifier les composants critiques ; renforcer les compétences techniques internes ; réaliser des audits réguliers et critiques des systèmes ; corriger les failles des systèmes de gestion de l'information ; établir un tableau de bord recensant les forces et les faiblesses du dispositif ; mettre en place des pare-feu robustes ; vérifier l'architecture globale des réseaux. Le panel a déploré l'absence d'un écosystème dynamique, adapté aux besoins de la jeunesse malienne.

3.2. Résumé des exposés :

Force est de reconnaître que le Mali consent des efforts colossaux dans la consolidation de la cyberdéfense. C'est à ce titre que le ML-CERT a vu le jour en 2023. Cette structure joue un rôle essentiel dans la lutte contre la cybercriminalité et la protection du cyberspace malien. Le ML-CERT, mis en place par l'AMRTP (Autorité Malienne de Régulation des Télécommunications/TIC et Postes), fonctionne comme une unité de gestion nationale dédiée à la cybersécurité à ce stade. Il doit être consolidé, renforcé et entièrement opérationnel sur tous les plans.

Les experts également évoqué les infrastructures critiques qui se définissent comme un ensemble d'installations, de réseaux ou de systèmes essentiels au bon fonctionnement d'une société. Leur indisponibilité ou dysfonctionnement peut avoir des conséquences majeures sur la sécurité des réseaux et des installations, aussi bien dans les secteurs publics que privés, et ce, dans plusieurs domaines clés.

Comme exemples concrets d'infrastructures critiques, on peut noter les centres de données, les systèmes boursiers, le secteur de l'énergie, les hôpitaux et les réseaux électriques.

Les risques auxquels ces infrastructures sont exposées en cas de cyberattaques sont majeurs : blocages dans différents secteurs, dysfonctionnements dans les services essentiels, et perte de données sensibles, notamment des données privées et perte économique.

À ce sujet, un recensement serait en cours de finalisation pour les identifier et les protéger du mieux possible. Le panel a déploré le fait que le Mali, à ce jour, ne dispose pas encore d'une stratégie de cybersécurité officielle en vigueur. Mais l'espoir est permis car le Ministère en charge des TIC et l'Autorité de régulation sont à l'œuvre en collaboration avec toutes les parties prenantes pour l'adoption d'une Stratégie Nationale de Cybersécurité.

Bien que ce document de stratégie n'ait pas été adopté, les experts y ont relevé l'absence de définition précise des infrastructures critiques ce qui est un manquement à combler.

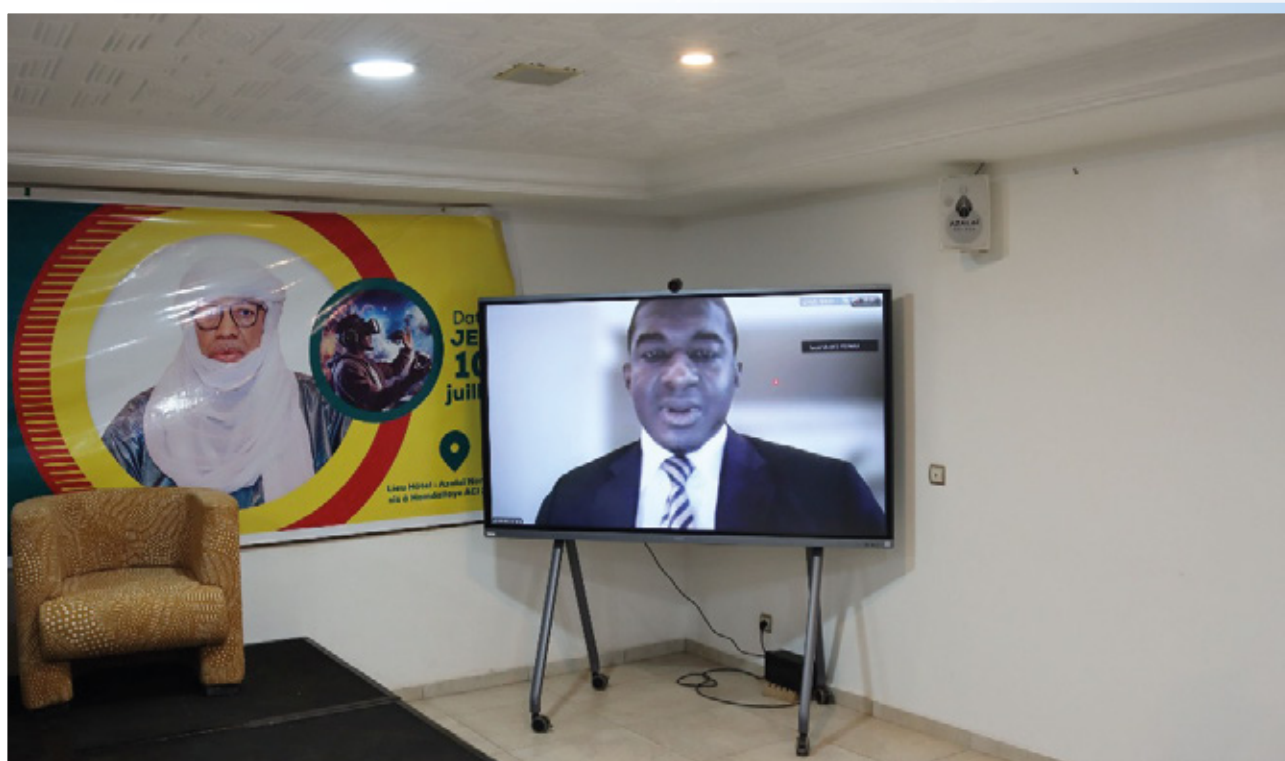
Le panel a également alerté sur les risques croissants d'attaques informatiques visant la population et les entreprises dans les jours à venir.

Sur la gestion des informations et la sécurité numérique, le panel a insisté sur la nécessité d'instaurer une véritable culture de cybersécurité. Cela passe par une large sensibilisation de la population, une élaboration de stratégies éducatives adaptées aux risques liés aux usages des appareils connectés, la formation continue, la démocratisation de l'accès à la cybersécurité et l'usage responsable et efficient de l'Internet, en particulier par les jeunes, pour qui le numérique représente un outil à double tranchant : à la fois une opportunité et un danger.

Concernant l'intelligence artificielle (IA), c'est un outil qui présente d'énormes défis de nos jours. Elle peut devenir un levier important pour renforcer la cybersécurité si elle est bien utilisée mais en même temps, elle est aussi utilisée pour mener des attaques très sophistiquées. Le panel a insisté sur la nécessité d'une sensibilisation en matière l'éducation numérique. Cela permettrait notamment d'apporter des solutions concrètes et rapides aux menaces numériques, de vérifier la fiabilité des sources d'informations, de booster les capacités du secteur numérique et de faciliter la mise en oeuvre de systèmes intelligents de protection.

Si l'IA offre des capacités avec lesquelles l'humain ne peut rivaliser, elle peut également présenter des comportements anormaux ou imprévisibles. Cela appelle à une vigilance, non seulement de la part de la société civile, mais aussi de l'État et du secteur privé quant à son utilisation.

En conclusion, le panel souligne la nécessité d'une volonté politique forte, accompagnée de politiques sectorielles claires et de moyens concrets pour mettre en oeuvre des actions efficaces en matière de cybersécurité.





Panel 4 : Données personnelles et vie privée à l'ère des technologies émergentes : quels enjeux pour la jeunesse et l'égalité de genre ?

4.1. Principaux points soulevés :

Au cours de ce débat, les principaux points suivants ont été soulevés.

Le manque de repère des femmes et des jeunes

De nos jours, la jeunesse et les femmes en particulier, bien qu'elles soient très actifs sur les plateformes numériques, manquent de repères. Nombreuses sont celles qui y arrivent désorientés ne sachant pas où aller ni quoi faire. Elles se laissent guider par la passion de scroller et se trouvent soudainement piégées. C'est cela qui explique le fait qu'elles soient les plus vulnérables. L'utilisation des réseaux sociaux est devenue un effet de mode et un lieu d'expression et de manifestation de tout ce qui est mal perçu dans les sociétés traditionnelles. Pour certains, les réseaux constituent juste un refuge.

Le rôle crucial de l'Autorité de Protection des Données à caractère Personnel (APDP)

En tant que régulateur, l'APDP joue un rôle clé dans la protection des données à caractère personnel. La problématique des données à caractère personnel et des données sensibles reste une préoccupation majeure dans un pays où l'autorité en charge est méconnue des utilisateurs.

L'APDP doit entreprendre des actions de communication, de sensibilisation surtout au niveau des responsables de traitement dans les organisations pour que la problématique puisse être comprise dans toutes ses dimensions. Cela permettra d'outiller les citoyens et les institutions en matière de gestion des données.

Dépravation des mœurs à travers des pratiques malsaines

Le panel a fait écho au développement des réseaux criminels qui ont pour activités principales l'exploitation des femmes, notamment par la diffusion de leurs profils sur des plateformes à leur insu et à des fins frauduleuses.

Dans la même veine, plusieurs utilisatrices ont vu certaines de leurs vidéos volées sur leurs propres comptes et utilisées à d'autres fins par ces cybercriminels. Plusieurs témoignages ont été recueillis lors du panel. L'APDP œuvre actuellement à identifier et à poursuivre ces cybercriminels.

La protection des données à caractères personnels comme défi pour les autorités

De nos jours, la protection des données à caractère personnel pose beaucoup de défis. Le Mali n'est pas en marge des initiatives dans ce domaine avec la loi de protection des données personnelles adoptée en 2013, la création de l'Autorité de protection, la création du Pôle judiciaire pour la cybercriminalité, mais reste encore beaucoup à faire .

Le panel a abordé l'impact des textes juridiques actuels, parfois en déphasage avec les réalités sociales et technologiques maliennes.

Le développement fulgurant de l'intelligence artificielle change la donne mondiale ce qui accroît la responsabilité des plateformes dans la gestion des données à caractère personnel. Par conséquent, les autorités doivent renforcer l'arsenal juridique en prenant en compte ces nouveaux aspects.

La préservation de la vie privée comme enjeu pour les utilisateurs :

L'exposition aux technologies a induit la migration de la société vers une société fortement digitalisée. Les objets connectés en l'occurrence les smartphones sont devenus nos compagnons les plus fidèles gardant tous nos secrets.

Par ailleurs, le panel a mis l'accent sur le lien étroit entre les nouvelles technologies et l'exploitation des données à l'insu des utilisateurs. Ainsi nous sommes exposés à des risques majeurs de violation de confidentialité tous les jours. Il revient aux utilisateurs de faire preuve de vigilance quant à leur vie privée en ligne. Le panel a mis en lumière que chaque individu est le maître de ses données, de sa vie privée. Pour ce faire il doit être bien informé pour pouvoir contrôler et limiter ce qu'il publie ou partage en ligne. À cet effet la formation et la sensibilisation sont indispensables.

4.2. Résumé des exposés :

Le panel a défini les données à caractère personnel comme étant toute information permettant d'identifier une personne de manière directe ou indirecte qu'il s'agisse d'un nom, d'une adresse IP, d'une photo ou même d'un identifiant numérique.

Ces données sont protégées par des textes en vigueur au Mali et ailleurs. Actuellement l'APDP est en train de traiter de nombreux cas de chantage et d'atteintes à la vie privée au Mali. Face à la prolifération de ces incidents, le panel a rappelé que personne n'est à l'abri des risques numériques. L'APDP agit à travers la sensibilisation, la régulation et les sanctions. Par ailleurs, le panel a encouragé les acteurs à soumettre systématiquement leurs conditions générales de collecte et de gestion à l'Autorité de protection pour validation.

Sur la question de la vidéosurveillance, l'APDP a mis en place des normes réglementaires par délibération, encadrant strictement l'installation de caméras dans les lieux publics et privés. Des clarifications ont été données concernant le caractère obligatoires des déclarations réglementaires au niveau de l'APDP avant toute installation par des tiers.

L'insouciance des jeunes vis-à-vis de l'usage de leurs données personnelles a été soulignée. La jeunesse aujourd'hui prend à la légère les dangers liés au téléchargement d'applications tout type, à l'usage de l'intelligence artificielle, ou encore à l'auto-exposition volontaire sur les réseaux sociaux, souvent sans aucune maîtrise des paramètres de confidentialité des appareils qu'ils utilisent.

La création d'une plateforme d'information en langues nationales afin d'accompagner les jeunes et les femmes dans un usage responsable du numérique pourrait être d'une très grande utilité surtout en milieu rural. Pour une sensibilisation massive, il serait pertinent d'intégrer l'éducation numérique dans les programmes scolaires, notamment pour prévenir les cas des harcèlements en ligne.

Le genre n'est pas resté en marge dans ce panel qui a mis en avant la présence massive des femmes en ligne mais qui a constaté également qu'elles sont les plus exposées. Les femmes sont vulnérables sur la toile et courent des risques de publication non consentie de leurs données personnelles, ce qui peut avoir des conséquences graves sur leur image, leur moralité et leur avenir professionnel. Mais malgré tout cela, les femmes constituent un maillon important de l'écosystème numérique. Elles doivent être formées, sensibilisées aux enjeux liés à leurs traces numériques.





Panel 5 : L'IA au service de l'innovation technologique et de l'entrepreneuriat numérique : défis, enjeux et perspectives

5.1. Principaux points soulevés

Ce panel a soulevé les principaux points suivants :

De l'informatique traditionnelle à l'IA :

L'informatique traditionnelle fait appel aux algorithmes classiques. L'algorithmique classique consiste à soumettre des instructions à l'ordinateur pour exécution. Par ailleurs, pour confier à l'ordinateur des tâches qui auparavant étaient dévolues aux êtres humains, il a fallu développer d'autres techniques basées sur les données. Cette fois, on transmet des données (informations) à l'ordinateur pour lui permettre d'apprendre des choses en toute autonomie. Une fois bien entraîné il va être capable de décider de certaines choses sans intervention humaine. C'est le principe de base de l'intelligence artificielle.

L'importance de l'IA

De nos jours, l'IA est incontournable. Elle s'impose à tous et dans tous les domaines. Les entreprises n'utilisant pas l'IA se trouveront rapidement hors de la compétition. Malheureusement beaucoup pensent que l'usage de l'IA se limite à ChatGPT ou à d'autres agents conversationnels (Chatbots) alors que l'IA a tout révolutionné: la GRH, la gouvernance, l'éducation, la santé, bref la technologie elle-même.

L'IA aurait-elle des inconvénients ?

Nous savons tous que l'IA est basée sur des données en grande quantité. Supposons que ces données ayant permis à une IA d'être entraînée soient erronées, cette IA prendra des décisions aussi erronées et ce qui engendrera tous les autres inconvénients. Selon le modèle et les types de données d'entraînement, l'IA peut fournir des informations qui ne sont pas en adéquation avec notre contexte. Pour pouvoir en tirer profit, nous devons adapter les IA à notre contexte. Une IA pourrait aussi avoir des biais algorithmiques qui peuvent être à la base de décisions erronées.

C'est pour cela que la norme ISO 42001 qui fournit aux organisations un cadre structuré pour développer, mettre en œuvre, maintenir et améliorer leurs initiatives d'IA de manière responsable, éthique et sécurisée, est très importante.

Les problématiques de l'utilisation ou freins de l'IA

La problématique de l'utilisation est due à l'analphabétisme numérique. L'inadaptation des contenus également a beaucoup favorisé cela. C'est pour cela que des initiatives comme Lenali conçue et développée au niveau local doivent être encouragées et soutenues.

Pour ce qui est des freins dans la mise en œuvre de l'IA, il faut souligner la crainte de se faire remplacer dans les entreprises. Une fois que les employés d'une entreprise pensent au fait qu'ils peuvent être remplacés par des outils (IA) qu'eux-mêmes mettent en œuvre cela pourrait créer une méfiance. Nous pouvons encore une fois parler des biais algorithmiques qui peuvent être dus aux données d'entraînement de l'IA. Nous ne pouvons pas ne pas parler du manque de transparence dans le traitement des données par l'IA qui constitue aussi un autre frein.

5.2. Résumé des discussions

Le sujet de l'IA est très passionnant. Il révèle à la fois des aspects techniques et surtout des aspects de gestion et d'accompagnement. Dans les entreprises, les salariés doivent avoir l'assurance que l'IA ne vient pas pour les remplacer. Certaines entreprises ont eu recours à des solutions d'IA mais pour les utiliser, le personnel n'a pas joué franc-jeu par peur de se voir remplacé par l'outil. Il est d'une nécessité absolue de former, renforcer les capacités des managers pour qu'à leur tour ils puissent mieux sensibiliser et rassurer les employés concernant la protection de leur emploi.

Nous devons aller vers la formation des chefs d'entreprise, des employés chacun en ce qui le concerne, pour un meilleur usage et une meilleure exploitation de l'intelligence artificielle pour profiter grandement de son potentiel.

En d'autres termes, nous (utilisateurs) devrions savoir ce que nous voulons dans la panoplie d'outils qui nous sont soumis. Il va falloir que nous-mêmes développons nos propres solutions adaptées à nos contextes et à nos réalités pour mieux répondre à nos besoins.

IV. Recommandations

À la suite des différentes discussions (Keynotes, panels), plusieurs recommandations ont émergé les recommandations les plus pertinentes, ayant fait l'objet de délibération lors du forum, sont présentées ci-dessous et catégorisées par thématiques.

S'agissant de la Gouvernance de l'Internet face aux technologies émergentes : quel équilibre entre Régulation et Innovation

Le forum a formulé les recommandations suivantes :

1. Organiser des forums comme le Forum sur la Gouvernance de l'Internet au Mali pour construire ensemble une gouvernance lucide, équilibrée et audacieuse, à hauteur des défis quelles que soient les avancés des innovations technologiques.
2. Réunir tous les acteurs de la gouvernance de l'Internet ainsi que des experts clés en la matière pendant ces fora afin de proposer des solutions pouvant réduire l'impact des technologies de rupture.
3. Palier à l'impact des technologies disruptives sans freiner l'innovation ni entraver la gouvernance des solutions numérique émergeantes afin de rendre Internet plus résilient, robuste et ouvert à tous à l'échelle mondiale.

Concernant la Gouvernance de l'Internet : défis et perspectives pour un Internet ouvert accessible et résilient au MALI :

Le forum a formulé des recommandations suivantes :

4. Adopter une approche multipartite de la gouvernance de l'Internet et passer à l'action en impliquant activement l'ensemble des parties prenantes : institutions publiques, secteur privé, société civile, communauté éducative, et en particulier les jeunes et les femmes ;
5. Bâtir une culture du numérique solide, ancrée dans les valeurs de responsabilité et de citoyenneté par la sensibilisation dès le plus jeune âge ;
6. Mettre en œuvre les recommandations des précédents forums sur la gouvernance de l'Internet qui demeurent des cadres structurés de dialogue et de concertation autour des enjeux numériques au Mali ;
7. Démocratiser l'Internet et le rendre accessible à tous : Il s'agit de rapprocher les services numériques de la population, en particulier dans les zones reculées, et de réduire les coûts d'accès, encore trop élevés pour une grande majorité de citoyens ;

8. Elaborer une stratégie claire et inclusive, nécessaire pour réduire la fracture numérique. Cette stratégie devra s'appuyer sur les piliers tels que :

- le renforcement des **infrastructures**,
- la démocratisation de la **formation**,
- la diffusion de l'**information utile et fiable**,

9. Former toutes les couches sociales afin de prévenir les dérives liées à une méconnaissance ou à un usage non encadré du numérique ;

10. Appliquer les lois avec justesse et impliquer les institutions de contrôle : La mise en œuvre des textes réglementaires doit se faire de manière mesurée, en tenant compte des réalités spécifiques du pays ;

11. Promouvoir un engagement collectif pour un Mali numérique émergent : chaque acteur (public, privé, institutionnel ou citoyen) doit jouer pleinement son rôle pour que le Mali soit en mesure de bâtir une société numérique moderne, équitable et résiliente, porteuse d'espoir pour les générations futures ;

S'agissant de la souveraineté numérique face aux technologies disruptives : quelles stratégies pour les États :

Le forum a formulé les recommandations suivantes :

12. Affirmer une volonté politique forte en soutenant activement les entreprises TIC nationales, à travers des financements ciblés et durables, pour renforcer leur capacité à contribuer à la souveraineté technologique ;

13. Élaborer une stratégie nationale de souveraineté numérique, claire et inclusive, intégrant les volets essentiels : formation, infrastructures, régulation, innovation et cybersécurité ;

14. Structurer la gouvernance numérique en reprenant le contrôle et la gestion locale du domaine .ml et en en faisant un levier stratégique de souveraineté nationale ;

15. Définir un modèle de gestion clair et bien structuré dans lequel le rôle de chaque partie prenante sera bien déterminé ;

16. Renforcer les capacités humaines et techniques en créant davantage de centres de données souverains, en formant massivement des ingénieurs et des techniciens, et en requalifiant les professionnels existants dans des écoles spécialisées ;

17. Réguler efficacement le cyberspace en développant un cadre juridique clair et en définissant une vision nationale et régionale cohérente de la cybersouveraineté, en partenariat avec les institutions africaines ;

Concernant la Cybersécurité et la résilience des infrastructures critiques à l'ère des ruptures technologiques :

Le forum a formulé les recommandations suivantes :

18. Renforcer les programmes de formation et de sensibilisation à destination des citoyens afin de favoriser une prise de conscience collective des risques liés à une utilisation non sécurisée du numérique ;

19. Encourager les citoyens, en particulier les jeunes et les femmes, à vérifier systématiquement la fiabilité des sources d'information en ligne, en les outillant contre la désinformation et les contenus manipulés ;

20. Intégrer l'éducation numérique dans les programmes scolaires et extrascolaires pour développer une culture numérique responsable et critique dès le plus jeune âge ;

21. Mettre en place des synergies nationales et régionales et instaurer une coopération renforcée entre États afin de formuler une réponse collective, inclusive et coordonnée face aux menaces technologiques, notamment liées à l'IA ;

22. Déployer des outils de détection et de surveillance des flux malveillants pour anticiper, identifier et contrer efficacement les cybermenaces pesant sur les infrastructures critiques ;

23. Créer un environnement favorable à la détection, à la formation et à l'accompagnement des jeunes talents puis les impliquer activement dans le développement de la cybersécurité nationale ;

24. Affirmer une volonté politique forte au niveau de l'État pour impulser, coordonner et soutenir les politiques de cybersécurité et de résilience des infrastructures critiques.

Concernant les données personnelles et la vie privée à l'ère des technologies émergentes : quels enjeux pour la jeunesse et l'égalité de genre :

Le forum a formulé les recommandations suivantes :

25. Renforcer les campagnes de sensibilisation sur la protection des données personnelles, en ciblant prioritairement les jeunes et les femmes ;

26. Créer des plateformes d'éducation numérique accessibles et inclusives, en intégrant les langues locales pour toucher tous les publics ;

27. Encourager les utilisateurs à vérifier la nature et la fiabilité des plateformes numériques avant d'y partager leurs informations personnelles ;

28. Mettre en place un cadre de consentement clair et obligatoire, en exigeant des opérateurs numériques qu'ils informent les usagers de manière simple et transparente avant toute collecte de données ;

29. Donner à chaque citoyen le contrôle sur ses données en renforçant l'éducation numérique de façon continue dès le plus jeune âge ;

30. Adapter les textes juridiques existants pour tenir compte des évolutions rapides des technologies émergentes, notamment en matière de traitement des données et d'intelligence artificielle ;

31. Soutenir activement l'Autorité de protection des données personnelles (APDP), en renforçant ses moyens humains, techniques et financiers, et en encourageant la coopération entre les institutions concernées ;

S'agissant de l'IA au service de l'innovation technologique et de l'entrepreneuriat numérique : défis, enjeux et perspectives

Le forum a formulé les recommandations suivantes :

32. Restreindre ou interdire l'accès à certains usages de l'intelligence artificielle pour les enfants, en particulier ceux pouvant nuire à leur développement, à leur sécurité ou à leur intégrité psychologique ;

33. Former et sensibiliser les parents aux usages et aux risques de l'IA afin qu'ils puissent exercer un contrôle parental éclairé et accompagner leurs enfants dans un usage responsable ;

34. Promouvoir une utilisation de l'IA qui soit efficace, critique et éthique, en encourageant la vigilance face aux risques de manipulation, de dépendance ou de désinformation ;

35. Mettre à jour les cadres juridiques nationaux pour encadrer efficacement l'usage de l'intelligence artificielle, en intégrant les notions de transparence, de responsabilité et de protection des groupes vulnérables, notamment les enfants et les femmes.

Concernant l'IA et la cybersécurité : nouveaux pouvoirs, nouvelles responsabilités pour la Gouvernance de l'Internet

Le forum a formulé les recommandations suivantes :

36. Créer un observatoire national de l'intelligence artificielle chargé de surveiller, analyser et encadrer les usages de l'IA, en s'appuyant sur une gouvernance rigoureuse pilotée par des experts qualifiés.

37. Promouvoir la recherche scientifique et renforcer la coopération régionale avec les pays limitrophes afin de développer un Internet plus résilient, plus sécurisé et adapté aux enjeux de cybersécurité partagés.

38. Élaborer des cadres législatifs spécifiques pour l'intelligence artificielle, en adoptant des lois dédiées à sa régulation, dans le but de garantir un Internet inclusif, accessible à tous, et respectueux des droits humains.

V. Annexe

1. Données démographique

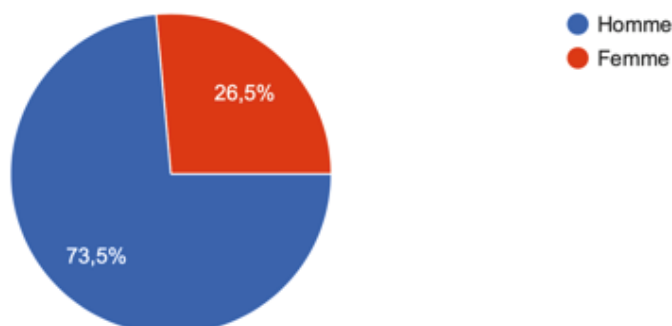
La 3ème édition du forum sur la gouvernance de l'Internet du Mali a enregistré une forte participation des différents acteurs. Le gouvernement, le secteur privé, la communauté technique et l'université étaient tous bien représentés. Des femmes comme des hommes ont répondu présent au nom des différentes parties prenantes. Le forum s'est déroulé en format hybride.

Pour la participation en salle, nous avons mis à disposition un QR code pour permettre aux participants de s'enregistrer. Ce QR code était disponible partout dans la salle.

Pour la participation en ligne, des participants comme des panelistes à distance se sont aussi inscrits sur Zoom afin de pouvoir prendre part à l'événement. Ces deux formulaires nous ont permis d'obtenir des informations démographiques sur la participation au forum. Ainsi, pour la participation en salle, nous avons enregistré 102 participants répartis comme suit :

En salle

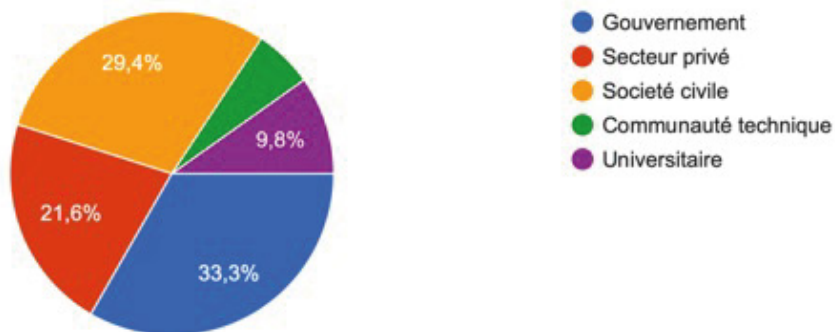
Etes-vous ?
102 réponses



Ces graphiques nous montrent que la majeure partie des participants était des hommes, avec 73,5 %. Les femmes étaient présentes à hauteur de 26,5 %.

A quelle partie prenante appartenez-vous?

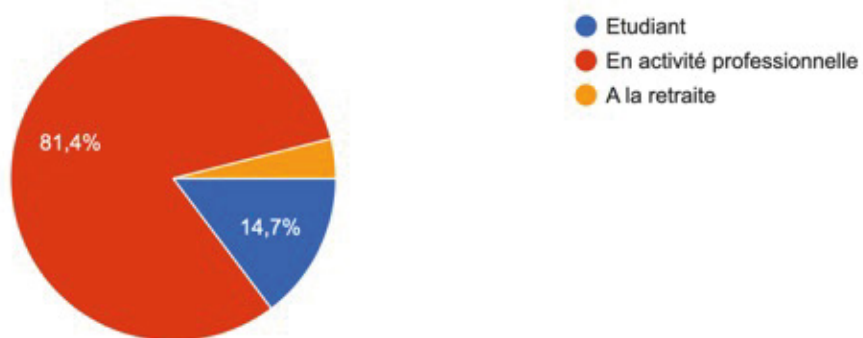
102 réponses



Concernant la représentativité des parties prenantes, le gouvernement était le secteur le plus représenté avec 33,3 %. Ensuite vient la société civile à hauteur de 29,4 %. Le secteur privé arrive en troisième position avec 21,6 %, suivi de l'université avec 9,8 %. La communauté technique était la moins représentée.

Quel est votre statut ?

102 réponses



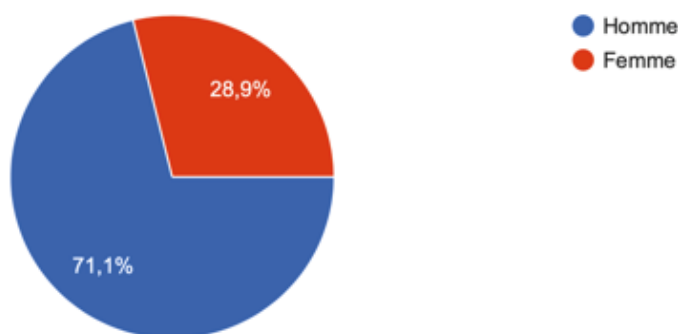
Les participants en activité professionnelle se sont davantage intéressés à l'événement avec 81,4 % de participation. Les étudiants représentaient 14,7 % des participants et le reste était constitué de retraités qui ont aussi manifesté un intérêt.

En ligne :

Le lien Zoom du forum a été diffusé lors de nos différentes communications sur l'événement. Nous avons eu des panélistes et des participants qui y ont pris part en ligne. Cela nous a permis de toucher un public intéressé qui n'a pas pu se déplacer sur le lieu du forum. Après l'extraction des données Zoom, nous avons enregistré 45 participants. Comme pour le formulaire Google, nous avons collecté les mêmes informations lors des inscriptions afin de faciliter les analyses.

Etes-vous ?

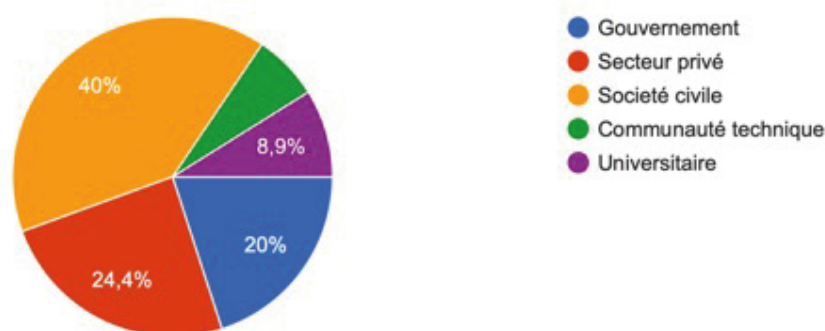
45 réponses



Ainsi, la participation en ligne a été dominée par les hommes avec un taux de 71,1%, contre 28,9% pour les femmes.

A quelle partie prenante appartenez-vous ?

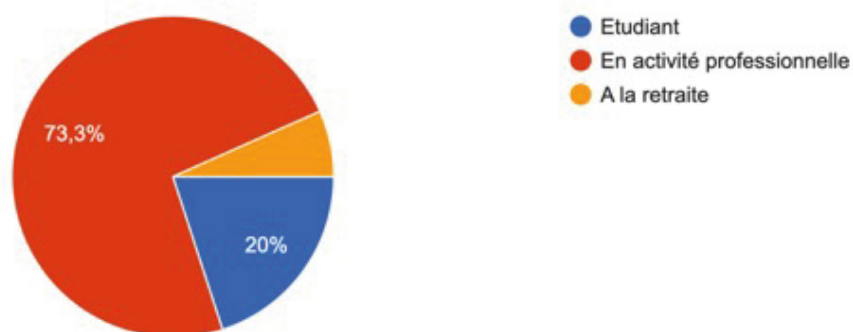
45 réponses



En ligne, la société civile a été la plus représentée avec un taux de participation de 40 %, suivie du secteur privé avec 24,4 %, contrairement à la participation en salle. Le gouvernement occupe le troisième rang avec 20 % et l'université avec 8,9 %.

Quel est votre statut ?

45 réponses

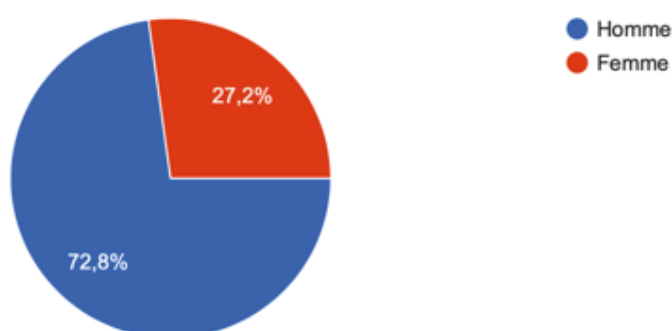


Comme pour la participation en salle, les participants en activité professionnelle ont été les plus nombreux, avec 73,3 %. Les étudiants ont occupé le deuxième rang avec 20 %. Des retraités étaient également présents en ligne

Globalement, le cumul des participants en salle et en ligne donne un total de 147 participants pour la 3^{ème} édition du forum malien sur la gouvernance de l'Internet. Cette édition du forum a enregistré en une seule journée un nombre de participants supérieur à celui des deux autres éditions précédentes. L'analyse globale de cette participation permet d'obtenir les graphiques suivants :

Etes-vous ?

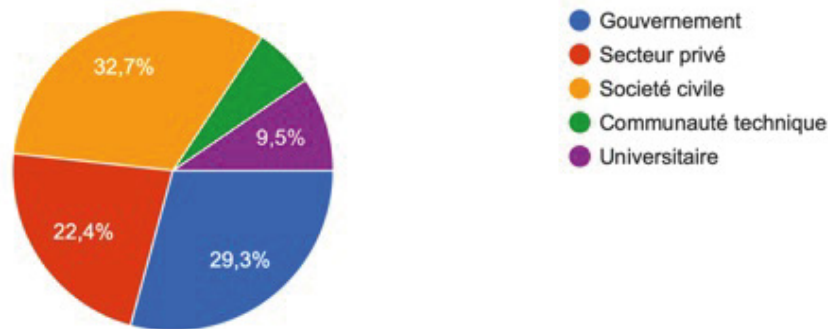
147 réponses



Globalement, la 3^{ème} édition du forum a enregistré 72,8 % d'hommes contre 27,2 % de femmes. Cette statistique montre clairement que nous devons fournir des efforts pour impliquer davantage les femmes dans le processus de la gouvernance de l'Internet au Mali. Ces dernières années, le chapitre s'est beaucoup concentré sur la formation des femmes et des jeunes filles, mais leur implication dans le processus de la gouvernance reste faible.

A quelle partie prenante appartenez-vous?

147 réponses

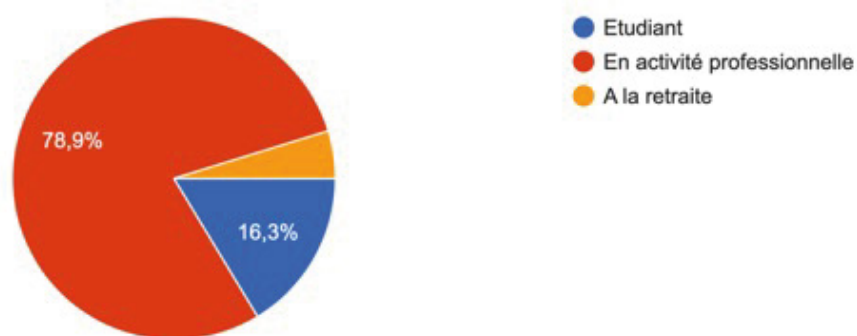


La société civile a été plus présente lors de cette 3e édition avec 32,7 %, suivie du gouvernement avec 29,3 % des participants. Le Secteur privé a répondu présent avec 22,4 % des participants. Comme à l'habitude, l'université et la communauté technique arrivent en dernière position.

Les trois parties prenantes principales à savoir la société civile, le Gouvernement et le secteur privé étaient presque équilibrées en terme de représentativité. Des efforts doivent être fournis concernant l'implication des universitaires et de la communauté dite technique.

Quel est votre statut ?

147 réponses



Les participants en activité professionnelle ont été majoritaires lors de ce forum. Les étudiants étaient présents, mais en moins grand nombre par rapport aux professionnels. Des retraités ont également participé.

2. Liste des intervenants



Liste des experts intervenus à la 3e édition du Forum sur la Gouvernance de l'Internet au Mali



Bakary Kouyate
Président d'ISOC MALI
/ FGI MALI



Abdrahamane Samba SIDIBE
Expert en Sécurité IP,
Membre du MAG FGI MALI



Ismaïla TOGOLA
Fondateur de ISMACORP
(Information Security
Management Corp)



Youssef SAKALY
DG ISERV MALI



Daly Hamady DIALLO
Président de l'Association
E-Citoyenneté (E-CIT Mali)



Ousmane FOMBA
Directeur Général de L'ANTIM
(Agence Nationale de Télésanté et
d'Informatique Médicale)



Aminata MAIGA
Cheffe de services Techniques à la HAC
(Haute Autorité de la Communication)



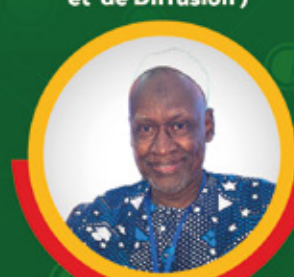
Bakary MAKAGUILE
Chef de Division Coopération
SMTD SA
(Société Malienne de Transmission
et de Diffusion)



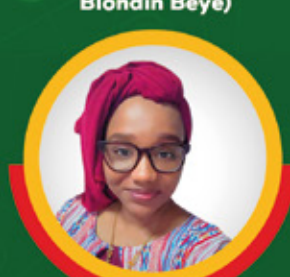
Col. Aliou BAGAYOKO
Directeur de l'instruction de
l'EMP-ABB (Ecole de
Maintien de la Paix Aliou
Blondin Beye)



Mohamadou Zarou
Conseiller du Président de l'AMRTP
(Autorité Malienne de Régulation des
Télécommunications, des TIC/Postes)



Dr Mamadou DIALLO Iam
Expert en stratégie de développement
TIC, Membre Fondateur d'ISOC MALI



Nana Salama Maïga
Consultante en
Système d'Informations

Liste des experts intervenus à la 3e édition du Forum sur la Gouvernance de l'Internet au Mali



Dr Mahamadou Aly HAIDARA
Directeur des Affaires Ju-
ridiques, du Contentieux et de la
Coopération à l'APDP
(Autorité de Protection des
Données à Caractère Personnel)



Assa SIMBARA
Experte en TIC et
Personne Ressource



Diabé BATHILY
Chef Unité de Recherche et de
Développement SMTD SA
(Société Malienne de
Transmission et de Diffusion)



Abdoulaye DOUCOURE
Expert Consultant en
Intelligence Artificielle



Fanta Coumba KAREMBE
Directrice Générale du SCSE (Service de
Certification et de Signature Electronique)



Dr Mamadou Gouro SIDIBE
Expert TIC, Président de
l'Association MALISTARTUP



Boua Ouarakoro Coulibaly
Coordinateur du ML-CERT
(Centre National de Réponse aux
Incidents de Cybersécurité)



Djimé SACKO
Tech Lead Kabakoo Academie



Assetou DIARRA
Présidente de l'Association
Femme & TIC Mali



Eric STEVANCE
Fondateur et Directeur
Général d'AFRIBONE



Youssef KEITA
Founder & CEO de KEITH CONSULTING

3. Agenda du forum

Horaire	Activité	Timing
7h45 - 08h00	Accueil et Installation des participants	15 min
8h00 - 08h15	Introduction du Forum	15 min
8h15 - 08h30	KeyNote1 : Gouvernance de l'Internet face aux technologies émergentes : quel équilibre entre Régulation et Innovation	15 min
8h30 - 10h00	Panel 1 : Gouvernance de l'Internet : défis et perspectives pour un internet ouvert accessible et résilient au Mali ?	1h30mn
10h00 - 10h20	Pause	20mn
10h20 - 11h00	Cérémonie d'Ouverture	40mn
11h00 - 12h30	Panel 2 (panel de haut niveau) : Souveraineté numérique face aux technologies disruptives : quelles stratégies pour les États ?	1h30mn
12h30 - 14h00	Panel 3 : Cybersécurité et résilience des infrastructures critiques à l'ère des ruptures technologiques	1h30mn
14h00 - 14h40	Pause	40mn
14h40 - 16h10	Panel 4 : Données personnelles et vie privée à l'ère des technologies émergentes : quels enjeux pour la jeunesse et l'égalité de genre ?	1h30mn
16h10 - 17h40	Panel 5 : L'IA au service de l'innovation technologique et de l'entreprenariat numérique : défis, enjeux et perspectives	1h30mn
17h40 - 18h00	Keynote 2 : L'IA et la Cybersécurité : nouveaux pouvoirs, nouvelles responsabilités pour la Gouvernance de l'Internet	20mn
18h00 - 18h15	Pause	15mn
18h15 - 18h45	Lecture des recommandations + Clôture	30mn

Activité	Speakers/Moderateurs/Paneliste
<p>KeyNote 1 : Gouvernance de l'Internet face aux technologies émergentes : quel équilibre entre Régulation et Innovation</p>	<p>Speaker : Abdrahamane Samba Sidibé</p>
<p>Panel 1 : Gouvernance de l'Internet : défis et perspectives pour un internet ouvert accessible et résilient au Mali ?</p>	<p>Modérateur : Bakary Kouyate Panélistes : Youssouf Sakaly, Daly Hamady Diallo, Nana Salama Maïga, Ousmane Fomba</p>
<p>Panel 2 : Souveraineté numérique face aux technologies disruptives : quelles stratégies pour les États ?</p>	<p>Modérateur : Bakary N Makanguile Panélistes : Colonel Aliou Bagayoko ; Mahamadou Zarou, Mamadou Diallo lam,</p>
<p>Panel 3 : Cybersécurité et résilience des infrastructures critiques à l'ère des ruptures technologiques</p>	<p>Modérateur : Eric Stevance Panélistes : Ismaël Togola ; Diabe Bathily Boua Ouarakoro Coulibaly</p>
<p>Panel 4 : Données personnelles et vie privée à l'ère des technologies émergentes : quels enjeux pour la jeunesse et l'égalité de genre ?</p>	<p>Modérateur : Assa Simbara Panélistes : Mahamadou Aly Haïdara ; Fanta Coumba Karembe, Assetou Diarra</p>
<p>Panel 5 : L'IA au service de l'innovation technologique et de l'entreprenariat numérique : défis, enjeux et perspectives</p>	<p>Modérateur : Aminata Maïga Panélistes : Dr Mamadou G Sidibé, Abdoulaye Doucouré ; Youssouf KEITA ; Djimé Sacko</p>
<p>KeyNote 2 : L'IA et la Cybersécurité : nouveaux pouvoirs, nouvelles responsabilités pour la Gouvernance de l'Internet</p>	<p>Keynote Speaker : Ismaël Togola</p>

Equipe de redaction

Astan Abdoulaye Traoré

Astan Kane

Fanta Coumba Karembe

Fatoumata Haidara

Fatoumata Nimaga

Karidia Sangaré

Lala Diallo

Bakary Kouyaté

Drissa Mariko

Mamadou Diallo IAM

Sawé Aminata Hélène DACKOOU

Awezou KOUYATE



<https://fgimali.ml>



info@fgimali.ml



[@fgimali](#)



[FGI_MALI](#)



[@fgimali](#)