



**CODESRIA**

## **INSTITUT SUR LA GOUVERNANCE DEMOCRATIQUE**

**Thème : Cybersécurité, souveraineté et gouvernance démocratique en Afrique**

**Date : 27 juillet – 07 août 2015**

**Lieu : Dakar, Sénégal**

**DATE LIMITE : 30 avril 2015**

### **Appel à candidatures : Session 2015**

Le Conseil pour le développement de la recherche en sciences sociales en Afrique (CODESRIA) a le plaisir d'annoncer la session 2015 de son Institut annuel sur la Gouvernance démocratique. Il invite les chercheurs à soumettre leurs candidatures à cet Institut devant se dérouler du **27 juillet au 07 août 2015** à Dakar (Sénégal).

Lancé en 1992 par le CODESRIA, l'Institut sur la gouvernance démocratique est un forum interdisciplinaire qui réunit chaque année une quinzaine de chercheurs venant des diverses régions du continent et de la diaspora, ainsi que des chercheurs non africains qui entreprennent des recherches innovantes sur des sujets liés au thème général de la gouvernance.

### **Organisation**

Les sessions de l'Institut sont dirigées par un directeur scientifique qui, avec le soutien de personnes ressources, s'assure qu'un large éventail de recherches et de questions politiques est exposé aux lauréats. Chaque lauréat doit rédiger un article découlant d'un travail de recherche destiné à être présenté durant l'Institut. La version révisée de l'article fera l'objet d'une évaluation par les pairs en vue de sa publication par le CODESRIA. Le Centre de documentation et d'information du CODESRIA (CODICE) mettra à la disposition des participants une bibliographie aussi complète que possible se rapportant au thème de l'Institut. Les participants auront également accès à des centres de documentation de Dakar et ses environs.

### **Langues**

La traduction simultanée sera disponible pendant l'Institut sur la gouvernance démocratique du CODESRIA qui se tiendra en français et en anglais.

### **Cybersécurité, souveraineté et gouvernance démocratique en Afrique**

La cybersécurité est le visage émergent de la sécurité à la fois dans la société de l'information et dans l'économie du savoir. Elle met en lumière un des phénomènes majeurs de la civilisation numérique qui se manifeste dans la forte dépendance vis-à-vis des systèmes d'information de notre mode de vie, de nos conditions de vivre et de notre sécurité. Ce phénomène semble aller de pair avec le développement fulgurant des technologies de l'information et de la communication ainsi que le décloisonnement des sphères publiques et

privées. Il s'agit là d'un phénomène global à dimension planétaire qui ne laisse indifférente aucune société, aucune organisation, aucune personne. Cette exigence de sécurité est inhérente au cyberspace vu comme un espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques. Mais au-delà de sa dimension technologique, la cybersécurité est dans une dialectique permanente avec notre réel dans sa double dimension matérielle et immatérielle.

Aujourd'hui, la cybersécurité nous interpelle de force à travers ce que les analystes appellent « les cavaliers de l'Apocalypse » de l'ère numérique : cybercriminalité, cyberterrorisme, cyberfraude, cyberattaques et cyberguerre. Ces cybermenaces qui se dressent comme des défis à l'humanité et à ses mécanismes de gouvernance ont fini de nous convaincre de la fragilité de nos politiques, de nos institutions, de nos infrastructures ainsi que de nos systèmes de défense et de sécurité. Elles peuvent poursuivre des objectifs malveillants comme l'espionnage, la déstabilisation des personnes et des organisations, le sabotage ou la destruction de systèmes d'information mais également le développement d'une psychose. Mais la cybersécurité répond également à nos besoins légitimes de protection lorsque nous faisons usage des technologies de l'information et de la communication pour découvrir, nous former, communiquer, jouer ou effectuer des transactions commerciales. L'actualité de l'année 2015 a été inaugurée par des atteintes à la cybersécurité et par des phénomènes de terrorisme qui s'appuient sur les technologies de l'information et de la communication mettant ainsi en visibilité les carences et les déficiences des systèmes de gouvernance de la sécurité.

Dans cet environnement marqué par une insécurité grandissante, la fracture numérique se creuse au détriment de l'Afrique en se banalisant à l'instar de la pauvreté. Le continent ne profite pas encore de tous les avantages du numérique mais il en subit, plus que tous, les travers. N'étant que consommateurs et non producteurs de technologies et de contenus, certains Etats et organisations d'Afrique s'excluent de la société de l'information, qui se veut pourtant inclusive, et ne participent que de façon marginale à l'économie du savoir.

Il n'est alors point surprenant de constater l'insuffisance des réponses africaines au besoin de sécurité dans le cyberspace, ce qui range une bonne partie du continent africain dans ce que l'on appelle les zones de paradis pénal ou cybercriminel. Malgré son retard technologique, l'Afrique cherche à se frayer un chemin dans l'univers numérique et cherche également à définir un cadre d'intervention pour l'ensemble des parties prenantes. Aussi a-t-elle, le 27 juin 2014 à Malabo, adopté une convention sur la cybersécurité et la protection des données à caractère personnel.

Si dans ce domaine le cadre juridique est utile et nécessaire, il doit toutefois être complété par une réflexion stratégique et prospective au service de l'effectivité de la Convention à travers son entrée en vigueur (après quinze ratifications) mais aussi de son efficacité, de son efficience et de sa durabilité.

Quelle est la situation de la gouvernance à l'épreuve des exigences de cybersécurité ? Quels sont les effets des atteintes à la cybersécurité sur la souveraineté numérique des organisations africaines, qu'elles soient publiques, privées ou sociétales ? L'Afrique est-elle à même de développer une capacité de réaction et de résilience face aux cybermenaces ? L'Afrique a-t-elle les moyens pour se forger sa propre vision en matière de cybersécurité et de l'assumer dans le cyberspace ?

Autant de questions qui interpellent les participants à la session 2015 de l'Institut sur la Gouvernance axée sur : « **Cybersécurité, souveraineté et gouvernance démocratique en Afrique** ».

L'objectif global de la session 2015 est d'analyser et d'anticiper l'évolution de la gouvernance confrontée aux enjeux et défis à la fois de la cybersécurité et de la souveraineté en Afrique.

Pour ce faire, elle offrira un cadre d'échanges favorable à la création d'un réseau de chercheurs africains qui serviront de relais pour l'éclosion de réponses africaines aux défis posés par la cybersécurité. Plusieurs objectifs spécifiques sont ainsi poursuivis par la session 2015:

- identifier les obstacles à la souveraineté numérique par la sécurisation du patrimoine numérique et technologique des Etats, des individus et des organisations (dépendance économique, manque d'initiatives nationales, déficit d'infrastructures nationales ...) et proposer des voies et moyens pour atteindre cette souveraineté numérique ;
- sensibiliser sur la nécessité de préserver les droits fondamentaux et les libertés publiques à travers notamment la protection des données à caractère personnel (définition d'un cadre juridique propice, promotion des initiatives sociales et étatiques pour y parvenir...);
- proposer des axes d'approfondissement des cyberlégislations africaines (liberté d'expression, propriété intellectuelle, protection et sécurité des enfants...) pour renforcer la confiance dans la société de l'information.

La session 2015 de l'Institut sur la gouvernance couvrira un large éventail de thèmes articulés autour des cinq axes suivants :

### **1. Etat des lieux et idées reçues sur la cybersécurité en Afrique**

- L'univers conceptuel : le concept de cybersécurité et les notions voisines et connexes (cyberterrorisme, cyberattaques, cybercriminalité, cyberguerre, cybermenaces, etc.) ;
- Référentiels africains en matière de cybersécurité ;
- Etat des lieux de la gouvernance en matière de cybersécurité (politique et stratégique ; économique et financière ; sociale et culturelle ; technologique, environnementale et juridique) ;
- Souveraineté numérique et cybersécurité ;
- Cybersécurité et contrôle des flux transfrontaliers ;
- Cybersécurité et tourisme ;
- Les économies de la cybersécurité ;
- Culture de cybersécurité dans les instances sociétales (école, associations, familles, etc.) ;
- Cybersécurité et traçabilité dans les réseaux sociaux.

### **2. Mutations et ruptures en matière de cybersécurité**

- Cybersécurité et technologies émergentes ;
- Cybersécurité et infrastructures critiques ;
- Cybersécurité et protection de l'identité numérique ;
- Cybersécurité et protection des données à caractère personnel ;

- Cybersécurité et libertés publiques ;
- Cybersécurité et protection des usagers des réseaux sociaux ;
- Cybersécurité et risques technologiques ;
- Cyberterrorisme et réseaux sociaux ;
- Cybersécurité et gouvernance électronique ;
- Cybersécurité et commerce électronique.

### 3. Scénarios du futur de la cybersécurité en Afrique

- Cybersécurité et gouvernance passive ;
- Cybersécurité et gouvernance réactive ;
- Cybersécurité et gouvernance préactive ;
- Cybersécurité et gouvernance proactive.

### 4. Les parties prenantes à l'écosystème de la cybersécurité

- Les acteurs étatiques (Etats, organismes publics)
- Les acteurs privés (producteurs de matériel, producteurs de contenus, commerçants, établissements de paiement, transfert d'argent, etc.) ;
- Les acteurs sociaux (individus, associations, réseaux, écoles, universités, groupes religieux, leaders d'opinion, etc.) ;
- Les CERT (*computer emergency response team*) et la cybersécurité ;
- Les autorités de certification et de normalisation ;
- Le traitement judiciaire de la cybercriminalité ;
- Les forces de l'ordre et de sécurité face à la cybercriminalité ;
- Les médias et le traitement de la cybersécurité ;
- Les autorités de régulation et la cybersécurité ;
- La coopération internationale face à la cybersécurité ;
- Cybersécurité et conditions et relations de travail.

### 5. Vers une vision africaine de la gouvernance de la cybersécurité

- Enoncé d'une vision africaine de la gouvernance en matière de cybersécurité ;
- Le socle éthique de la promotion de la cybersécurité en Afrique ;
- Les objectifs stratégiques de la promotion de la cybersécurité ;
- La contribution de l'Afrique à la lutte contre la cybercriminalité ;
- La contribution de l'Afrique à la lutte contre le cyberterrorisme ;
- Mise en place d'un réseau de recherche sur la cybersécurité et la gouvernance en Afrique.

#### Le Directeur

Le **Professeur Abdoullah Cissé**, expert en cyberdroit et cybersécurité, dirigera la session 2015 de l'Institut sur la Gouvernance démocratique. En tant que Directeur de l'Institut, il assurera les tâches suivantes :

- Participer à la sélection des lauréats et à l'identification de personnes ressources appropriées;

- Interagir avec les personnes ressources et les lauréats pour une préparation adéquate de l'Institut sur la gouvernance ;
- Concevoir les cours de la session, notamment les sous-thèmes spécifiques ;
- Faire une série de conférences et mener une analyse critique des communications présentées par les personnes ressources et les lauréats ;
- Rédiger et soumettre un rapport scientifique relatif à la session;
- Editer les versions révisées des communications présentées par les personnes ressources, en vue de leur publication dans l'une des collections du CODESRIA. Pour la publication, le Directeur devra également assister le CODESRIA dans l'évaluation des communications présentées par les lauréats au cours de l'Institut.

### **Les personnes ressources**

Les cours devant être dispensés durant l'Institut sont destinés à offrir aux lauréats l'occasion d'approfondir leurs réflexions sur le thème. Les personnes ressources doivent, par conséquent, être des universitaires ou des chercheurs confirmés qui ont beaucoup publié sur le sujet, et qui ont une contribution importante à apporter aux débats. Elles devront produire des supports écrits qui inciteront les lauréats à engager la discussion et le débat sur leur exposé ainsi que toute la documentation disponible sur le thème.

Une fois sélectionnées, les personnes ressources doivent :

- Interagir avec le directeur de l'Institut et les lauréats afin d'aider ces derniers à réajuster leurs questions de recherche et leurs approches méthodologiques ;
- Soumettre un exemplaire de leurs supports de cours pour reproduction et distribution aux participants au plus tard une semaine avant la présentation de leurs exposés ;
- Présenter leur exposé, participer aux débats et commenter les propositions de recherche et les articles des lauréats ;
- Réviser et soumettre un article basé sur leurs notes de cours pour publication par le CODESRIA, au plus tard deux mois après l'Institut.

### **Les lauréats**

Les candidats doivent être des étudiants en thèse ou des universitaires en début de carrière, ayant une capacité prouvée à faire de la recherche sur le thème de l'Institut. Les intellectuels actifs dans le processus politique et/ou dans les mouvements sociaux et les organisations de la société civile sont également encouragés à se porter candidats. Le nombre de places offertes par le CODESRIA pour chaque session est limité à quinze (15). Les chercheurs non-africains qui peuvent financer leur participation peuvent également faire acte de candidature sous réserve des places disponibles.

### **Les dossiers de candidature des personnes ressources**

Les dossiers de candidature des personnes ressources doivent comprendre :

1. Une lettre de candidature ;
2. Un curriculum vitae ;
3. Deux (2) articles publiés
4. Une proposition de cinq (5) pages au plus, décrivant les questions qui seront couvertes dans leurs **trois (3) exposés** dont un portant sur les questions de méthodologie ;

### **Les dossiers de candidature des lauréats**

Les dossiers de candidature des lauréats doivent comprendre :

1. Un formulaire de candidature dûment rempli ;
2. Une demande de candidature ;
3. Une lettre attestant de l'affiliation institutionnelle ou organisationnelle ;
4. Un curriculum vitae ;
5. Une proposition de recherche de dix (10) pages, comprenant une analyse descriptive du travail que le candidat veut entreprendre, un résumé exposant l'intérêt théorique du thème choisi par le candidat, la relation entre le sujet et la problématique et les centres d'intérêt pris en compte par le thème de l'Institut 2015 ;
6. Deux (2) lettres de référence provenant d'universitaires ou de chercheurs connus pour leur compétence et leur expertise dans le domaine de recherche du candidat (du point de vue géographique et concernant la discipline), avec leurs noms, adresses, numéros de téléphone et adresses électroniques.
7. Une copie du passeport.

### **Date limite de soumission des candidatures**

La date limite de soumission des candidatures est fixée au **30 avril 2015**. Les lauréats seront informés du résultat de la sélection dans la dernière semaine du mois de mai **2015**. Le mois de juin pourra ainsi être utilisé pour mener à bien un travail de terrain ou recueillir de l'information pour préparer le projet de rapport de recherches à présenter lors de l'Institut. Ce rapport de recherches devra être soumis au CODESRIA au plus tard le **15 juillet 2015**. Les lauréats seront appelés à travailler sur ce document (et non sur le résumé de la proposition) et le préparer pour publication au cours de l'Institut.

### **Soumission des candidatures**

Toutes les candidatures ou demandes de renseignements complémentaires devront être adressées de façon électronique à : [governance.institute@codesria.sn](mailto:governance.institute@codesria.sn) .

**Pour vos questions spécifiques, veuillez-vous adresser à:**  
**CODESRIA**

**INSTITUT SUR LA GOUVERNANCE DEMOCRATIQUE**

Avenue Cheikh Anta Diop x Canal IV

BP 3304, CP 18524, Dakar, Sénégal

Tél. : (221) 33 825 98 21/22/23 - Fax : (221) 33 824 12 89

Email: [governance.institute@codesria.sn](mailto:governance.institute@codesria.sn)

Website: <http://www.codesria.org/>

Facebook: <http://www.facebook.com/pages/CODESRIA/181817969495>

Twitter: <http://twitter.com/codesria>