AFRICAN FORUM ON CYBERCRIME

Policies and Legislation, International Cooperation and Capacity Building

Législation et politiques en matière de cybercriminalité au Sénégal

Dr. Papa Assane TOURE
Magistrat
Expert en Cyberdroit
Secrétaire général Adjoint du Gouvernement (Sénégal)

• Cadre stratégique des politiques de cybercriminalité

- Plan Sénégal Emergent (PSE 2035): la transformation structurelle de l'économie à l'horizon 2035
- L'adoption de la stratégie « Sénégal numérique 2025» (SN2025): TIC comme l'un des moteurs clés de cette transformation économique
- Elaboration de la « Stratégie nationale de Cybersécurité 2022 » (SNC2022): confiance numérique
- Vision stratégique: « En 2022 au Sénégal, un cyberespace de confiance, sécurisé et résilient pour tous ».

→ Objectif stratégique 1: renforcement le cadre juridique et institutionnel de la cybersécurité au Sénégal ;

→ Objectif stratégique 5 : participation aux efforts régionaux et internationaux de cybersécurité.

SENEGAL EMERGENT

• Le renforcement le cadre juridique et institutionnel de la cybersécurité au Sénégal

- **La mise en place d'un cadre juridique et institutionnel de lutte contre la cybercriminalité**: loi n° 2008-11 du 25 janvier 2008 portant sur la cybercriminalité

✓ *La création de nouvelles infractions spécifiques aux TIC*

- Les atteintes aux systèmes informatiques
  - Les atteintes aux données informatiques
  - Les infractions informatiques
  - La pornographie enfantine
  - Les actes racistes et xénophobes

✓ *L'adaptation des infractions classiques aux TIC*

- Escroquerie en ligne, vol d'information, diffamation en ligne, etc.

✓ *La consécration de la responsabilité pénale des personnes morales*

✓ *L'extension des pouvoirs d'investigation des autorités judiciaires*

- Perquisition, saisie électronique, conservation rapide de données, admissibilité de la preuve électronique, etc.

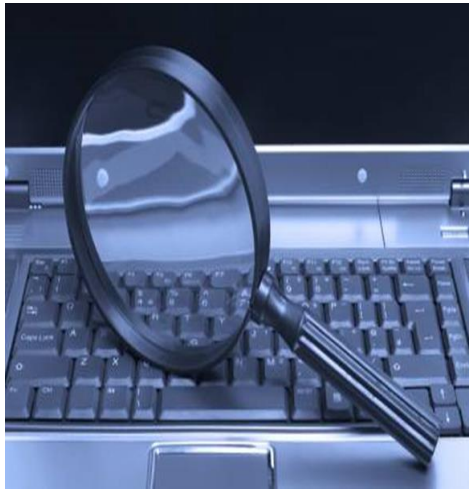
• Le renforcement le cadre juridique et institutionnel de la cybersécurité au Sénégal

- **L'application judiciaire du dispositif juridique**: près de 200 décisions de justice rendues
  - Interprétation de la notion de système informatique (TGIHC Dakar du 17 avril 2012, affaire du système WARI);
  - Définition de l'accès frauduleux (CA Dakar, n° 978 du 13 décembre 2010, Affaire Fulgence;
  - Précision apportées au concept de publicité en ligne (CA Dakar du 25 mars 2011, affaire Palluci).

- La création de structures d'investigation en matière de cybercriminalité
  - La Brigade spéciale de lutte contre la cybercriminalité (BSLC) devenue une Division spéciale de Cybersécurité (DSC);
  - La Section Recherche de la Gendarmerie: compétence nationale

• La mise à jour du cadre de lutte contre la cybercriminalité

- Réforme du Code pénal et du Code de Procédure pénale: loi n° 2016-29 et 2016-30 du 08 novembre 2016
- **La prévision de nouvelles infractions**
  - Le cyberterrorisme;
  - L'usurpation d'identité numérique;
  - Le copiage frauduleux de données;
  - La captation frauduleuse de l'image des personnes, etc.
- **L'institution de nouveaux moyens d'investigation**
  - L'injonction de produire;
  - Le blocage judiciaire de contenus manifestement illicites;
  - Les réquisitions de retrait de contenus manifestement illicites;
  - L'interception de correspondances émises par voie électronique, etc.



• La participation aux efforts régionaux et internationaux de cybersécurité

- Trois niveaux de coopération en matière de cybercriminalité :

✓ **Niveau sous régional**: transposition par référence de la Directive C/DIR/1/08/11 du 19 août 2011 portant lutte contre la cybercriminalité dans l'espace de la CEDEAO

✓ **Niveau continental**: la ratification de la Convention de Malabo du 27 juin 2014 sur la cybersécurité et la protection des données à caractère personnel (décembre 2016)

✓ **Niveau international**: l'adhésion à la Convention de Budapest du 23 novembre 2001 (décembre 2016)

- **Nations-Unies: l'absence d'un instrument juridique international**

- 12eme congrès des Nations Unies pour la prévention du crime et la justice pénale tenu à Salvador (Brésil) du 12 au 19 avril 2010: proposition d'adoption d'une convention internationale contre la cybercriminalité.

- Débat de l'adoption d'une convention internationale sur la cybercriminalité: ONUDC, réunion d'experts intergouvernementaux à Vienne du 10 au 13 avril 2017

- Absence d'un instrument juridique spécifique à la lutte contre la cybercriminalité au niveau des Nations Unies.

• L'articulation entre les Conventions de Malabo et de Budapest

- **Champs d'application différents des conventions** :
  - ✓ Domaine limité de la convention de Budapest: répression de la cybercriminalité
  - ✓ Domaine large de la convention de Malabo: cybercriminalité/ cybersécurité/ protection des données à caractère personnel, transaction électronique
- **Portées juridiques différentes des conventions**:
  - ✓ La Convention de Malabo: un traité continental: ratification par les Etats Membres de l'UA (art. 35 Convention Malabo):
  - ✓ La Convention de Budapest: un traité international: ouverte à l'adhésion de tous les Etats (art. 37 de la convention de Budapest)
- **Complémentarité des deux conventions** : les Etats parties s'engagent à se prévaloir des moyens régionaux et internationaux de coopération existants aux fins de répondre aux cybermenaces (art. 28 paragraphe 4 de la Convention)

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Questions