

AF-CYBERSEC 2008

« Conférence régionale africaine sur la cybersécurité  
« *Bâtir un espace numérique de confiance en Afrique* »

*Yamoussoukro, 17 au 20 novembre 2008*

## LA CYBERSECURITE : LES MOYENS JURIDIQUES DE PROTECTION

Abdoullah CISSE  
Professeur des universités, Sénégal  
Expert en droit des affaires et cyberdroit

# SOMMAIRE

- ENTRÉE EN MATIÈRE
- LES CINQ AXES DU DISPOSITIF DE PROTECTION JURIDIQUE

# SOMMAIRE

– La cybersécurité et le droit :  
quels problèmes juridiques ?

IV. La cybersécurité et le droit :  
quel dispositif de protection ?

# I - ENTRÉE EN MATIÈRE

LA CYBERSECURITE SAISIE PAR LE DROIT :  
DE QUOI ON PARLE ?

3. CONTEXTE

4. ENJEUX

5. DEFIS

6. OBJET

7. FINALITE

# ENTRÉE EN MATIÈRE – 1 - Contexte

- ➡ Globalisation des risques, des crimes et des menaces sur la cybersécurité
- ➡ Besoin de stratégies innovantes de politique criminelle combinant les réponses étatiques, sociétales et techniques
- ➡ Des efforts certains de protection juridique (nationale, communautaire et international)
- ➡ Un cadre peu propice à la cybersécurité, à améliorer

## LA CYBERSECURITE : DES ENJEUX MULTIPLES

- **S**CIENTIFIQUE
- **T**ECHNOLOGIQUE
- **E**CONOMIQUE ET FINANCIER
- **P**OUVOIR (politique au sens large)
- **S**OCCIO-CULTUREL (humain)

# ENTRÉE EN MATIÈRE – 2- Enjeux

## LA CYBERSECURITE : DES ENJEUX COMPLEXES

- La sécurité informationnelle touche à la sécurité du **patrimoine numérique et culturel** des individus, des organisations et des nations.
- La vulnérabilité dans le fonctionnement normal des Institutions peut compromettre la **pérennité et la souveraineté des Etats**.
- La prise en charge de la cybersécurité requiert une **volonté politique** clairvoyante pour :
  - ❖ définir et réaliser une stratégie de développement des infrastructures et services du numérique (e-services)
  - ❖ articuler avec une stratégie pluridisciplinaire de la cybersécurité cohérente, efficace et contrôlable

# ENTRÉE EN MATIÈRE – 3- Défis

- Obtenir un niveau de **sécurité technologique** suffisant pour prévenir et maîtriser les risques technologique et informationnel
- Edification d'une société de l'information respectueuse des **valeurs**, protectrice des **droits et libertés**, garantissant la sécurité des biens des personnes, des organisations et des nations
- Contribution à l'économie du savoir en garantissant un accès égal à l'information, en stimulant la création de **savoirs conformes**.

# ENTRÉE EN MATIÈRE – 3- Défis

## CREATION D'UN **ENVIRONNEMENT DE CONFIANCE**

- 👉 **Prévisible** : prévention et règlements des différends/  
Evolutif : tenant compte de l'évolution technologique continue
- 👉 **Organisé** : tous les secteurs pertinents
- 👉 **Protecteur** : des consommateurs et de la propriété intellectuelle (civile et pénale), des citoyens, des organisations, des nations
- 👉 **Sécurisé** : adéquation sécurité juridique et technologique
- 👉 **Intégré** à l'ordre international : articulation entre le national, le régionale et le mondial

## **Objet de la cybersécurité :**

➡ Contribuer à préserver les forces et les moyens organisationnels, humains, financiers, technologiques et informationnels, dont se sont dotées les Institutions, pour réaliser leurs objectifs.

➡ Englobe le traitement de la cybercriminalité mais ne se limite pas cet aspect.

## Finalité de la cybersécurité :

- ➡ Protéger les institutions contre les **menaces** et les **préjudices** pouvant mettre en péril leur pérennité et leur efficacité.
- ➡ Protéger les droits des **personnes** lors de la collecte, le traitement des données contre les menaces et es préjudices pouvant les affecter.
- ➡ Limiter les **atteintes ou dysfonctionnements** institutionnels induits, en cas de sinistre.
- ➡ Autoriser le retour à un **fonctionnement normal** à des coûts et des délais raisonnables.
- ➡ Mettre en place des mécanismes juridiques et institutionnels susceptibles de garantir **l'exercice normal** des droits humains dans le cyberspace.



**FIN ENTREE EN MATIERE**



**ETAPE SUIVANTE :**

**la cybersécurité et le droit :  
quel dispositif de protection ?**

## II - DU DISPOSITIF DE PROTECTION JURIDIQUE

LA CYBERSECURITE : QUEL DISPOSITIF JURIDIQUE ?

### LES CINQ AXES

- **UNE POLITIQUE DE CYBERSECURITE**
- **UNE CYBERETHIQUE**
- **UN CYBERDROIT PENAL**
- **UNE PROCEDURE PENALE ADAPTEE**
- **DES INSTITUTIONS APPROPRIEES**

## ➡ Définir une **véritable politique de sécurité**

- qui énonce ses exigences de sécurité envers les utilisateurs (acteurs, partenaires, prestataires) des nouvelles technologies,
- sur la base d'une approche globale, pluridisciplinaire et systémique de la sécurité.

➔ Définir un **périmètre de sécurité** basé sur :

- ❖ Une identification correcte des valeurs, des personnes, des organisations et des biens à protéger
- ❖ Une politique criminelle de **modernisation** du droit et de la procédure en tenant compte de l'impact des Tic sur les phénomènes juridiques
- ❖ Une politique de **sauvegarde** des valeurs fondamentales de la société
- ❖ **L'adoption** de nouvelles incriminations et **l'adaptation** des incriminations traditionnelles

- ➡ Articuler les **réponses étatiques, sociétales et techniques** devenues complémentaires et interdépendantes
- ➡ Mettre en place des **mesures de sécurité** adaptées tant sur le plan technique que juridique pour tenir compte par exp des diverses formes de cyberattaques
- ➡ Savoir que des solutions sécuritaires d'ordre uniquement technologique ne peuvent pas suppléer à un manque de **gestion** cohérente et rigoureuse des besoins, mesures, procédures et outils de la sécurité.

- Promouvoir et développer un **comportement cohérent, responsable et raisonnable** vis-à-vis des technologies de l'information
- Incompatibilité de la cybersécurité avec un monde **libertaire**, fluide et non contrôlé.
- Nécessité d'établir des grands principes **d'éthique, de responsabilité, de transparence**
- Consacrer les valeurs dans un **cadre légal approprié** ; national/communautaire/international
- Mettre en vigueur **des règles du jeu réalistes** qui soient applicables non seulement localement mais aussi par l'ensemble de la communauté internationale et compatibles avec les directives internationales existantes.

## • PROBLEMES

- Émergence de **nouvelles formes de délinquance informatiques** qui utilisent l'informatique comme **moyen** pour commettre des délits classiques ; comme **but** de la criminalité en s'attaquant aux systèmes d'information; comme **support** de la criminalité pour commettre des atteintes sexuelles sur les mineurs, des infractions de presse, de racisme etc.
- Absence d'un **cadre institutionnel** adéquat pour traiter des atteintes
- Absence de **responsabilité pénale** pour les personnes morales
- Risque de pillage des œuvres protégées par la propriété intellectuelle
- Risque d'atteintes aux **droits des personnes** dans le cadre de la collecte et du traitement des données personnelles
- **Déséquilibre informationnel** entre la personne et les entreprises et administrations qui traitent l'information

## • SOLUTIONS

- ➔ Criminalisation et pénalisation de :
  - l'accès illégal à un système d'information
  - Les atteintes à la confidentialité et à la disponibilité des données et systèmes d'information
  - Les infractions informatiques
  - Les infractions se rapportant aux contenus

## • SOLUTIONS

- ➡ Consécration de la responsabilité pénale des personnes morales
- ➡ Limitation du droit des responsables des traitements dans la collecte, l'utilisation et la transmission des données à caractère personnel
- ➡ Consécration de nouveaux principes et droits pour assurer la transparence des traitements opérés sur l'information
- ➡ Protection pénale des droits de propriété intellectuelle

# PROBLEMES

- Inadaptation des règles de procédure pénale à la recherche de la preuve, à la saisie informatique et télématique
- Risque d'atteinte aux droits fondamentaux dans la recherche de l'efficacité de l'enquête

## SOLUTIONS

- Actualiser la procédure pénale à la lumière des TIC
- Mise en place d'un système d'expertise pour la recherche de la preuve dans les systèmes informatiques et création d'un centre d'expertise et de lutte contre la cybercriminalité (décret)
- Concilier entre les exigences de l'efficacité de l'enquête pénale et le respect des droits fondamentaux
- Développer la coopération judiciaire et policière et entre autorités de régulation.
- Adhérer à la convention du Conseil de l'Europe sur la cybercriminalité.

- ➡ Mettre en place des instances consultatives, de veille et de prospective stratégique sur la cybersécurité
- ➡ Création d'une autorité administrative indépendante pour garantir le respect des principes et droits consacrés
- ➡ Mise en place :
  - d'infrastructure de confiance pour le commerce électronique (accréditation, certification, normalisation)
  - des instances **de justice et de police** compétentes dans le domaine des nouvelles technologies et capables de coopérer au niveau international avec leurs homologues;
  - la création de centre d'expertise sur la cybercriminalité.



**MERCI DE VOTRE ATTENTION !**

**Abdoullah CISSE**  
*Professeur des universités*  
*Expert en droit des affaires et cyberdroit*  
Pour vos observations mail to :  
[acissea@gmail.com](mailto:acissea@gmail.com)