



AF-CYBERSEC 2008

**«African regional Cybersecurity Conference
«Towards a Safe Cyberspace in Africa»**

Yamoussoukro, 17 to 20 November 2008

CYBERSECURITY : LEGAL INSTRUMENTS OF PROTECTION

Abdoullah CISSE
*University Lecturer, Senegal
Business and Cyber Law Expert*

CONTENT

II. INTRODUCTION

**III. THE FIVE COMPONENTS OF THE
LEGAL PROTECTIVE SYSTEM**

CONTENT

- I. Cybersecurity and Law :
Which Legal Problems?
- II. Cybersecurity and Law :
Which protective System?

I - INTRODUCTION

CYBERSECURITY AS A LEGAL CONCERN:
WHAT IS IT ABOUT?

3. CONTEXT

4. STAKES

5. CHALLENGES

6. SUBJECT

7. OUTCOME

INTRODUCTION – 1 - Context

- ➡ Globalizing risks, crimes and threats to cybersecurity
- ➡ Need of innovative criminal policy strategies mainstreaming governmental, societal and technical responses
- ➡ Effective legal protection initiatives (national, community-based and international)
- ➡ Poor cybersecurity environment to be improved

INTRODUCTION – 2- Stakes

CYBERSECURITY : MULTIPLE STAKES

- **S**CIENTIFIC
- **T**ECHNOLOGICAL
- **E**CONOMIC AND FINANCIAL
- **A**UTHORITIES (political in general)
- **S**OCCIO-CULTURAL (human)

INTRODUCTION – 2- Stakes

CYBERSECURITY : COMPLEX STAKES

- Information security addresses the security of **digital and cultural assets** of individuals, organizations and nations.
- Vulnerability in normal operations of institutions can compromise the **sustainability and sovereignty of States..**
- Cybersecurity management requires intelligent **political will** to:
 - ❖ develop and implement an infrastructure and digital service (e-services) development strategy
 - ❖ be in phase with a multi-pronged strategy on consistent, effective and controllable cybersecurity

INTRODUCTION – 3- Challenges

- Reaching a reliable level of **technology security** to prevent and control technology and information-related risks
- Building an information society that complies with **values**, protects **rights and liberties**, guarantees safety of life and property, organizations and nations
- Contributing to knowledge economy by ensuring equal access to information, and fostering creation of **standard knowledge**.

INTRODUCTION – 3- Challenges

CREATION OF **A SAFER ENVIRONMENT**

- 👉 **Preventive**: dispute prevention and settlement / Evolutionary: takes into account the continual technological evolution
- 👉 **Organized** : all relevant sectors
- 👉 **Protective** : for consumers and the intellectual property (civil and criminal), citizens, organizations and nations
- 👉 **Secured** : adequacy between legal and technological security
- 👉 **Integrated** in the International Order: Links national, regional and global levels

Objective of Cybersecurity:

- ➡ To contribute to preserve organizational, human, financial, technological and informational means and potentials in Institutions, to achieve their goals.
- ➡ Addresses Cybercrime issues but is not limited to this aspect.

INTRODUCTION– 5- Goal Object

Cybersecurity ultimately aims at:

- **Protecting** institutions against **threats** and **prejudices** likely to compromise their sustainability and effectiveness.
- **Protecting** the rights of **people** during data collection and processing against threats and prejudices that can affect them
- **Limiting** institutional **damages or malfunction** in the event of a disaster.
- **Authorizing** the return to **normal operations** at reasonable costs and time.
- **Setting up** legal and institutional mechanisms that can guarantee the **normal practice** of human rights in cyberspace.



INTRODUCTION (END)



NEXT STEP:

**Cybersecurity and Law:
Which protective system?**

II – LEGAL PROTECTIVE SYSTEM

CYBERSECURITY : WHICH LEGAL SYSTEM?

THE FIVE COMPONENTS

- **A CYBERSECURITY POLICY**
- **CYBERETHICS**
- **A CYBER CRIMINAL LAW**
- **AN APPROPRIATE CRIMINAL PROCEDURE**
- **APPROPRIATE INSTITUTIONS**

Defining a **real security policy**

- which displays its security requirements to new technology users (actors, partners, service providers),
- based on a global, multidisciplinary and systemic security approach.

- ➔ Defining a **security perimeter** based on:
- ❖ An correct identification of values, people, organizations and goods to be protected
 - ❖ A criminal policy of **modernization** of law and procedures taking into account the impact of ICTs on the legal phenomena
 - ❖ A policy for **safeguarding** basic societal valuesé
 - ❖ The **adoption** of new incriminations and the **adaptation** of the traditional incriminations

- Articulating **government, societal and technical** responses that have become complementary and interdependent
- Establishing appropriate **security measures** on at technical and legal levels to address all forms all cybercrime
- Understanding that security solutions applied to technology only cannot bridge the gap of consistent and rigorous **management** of the security-related needs, measures, procedures and tools.

- Promoting and developing a **consistent, responsible and reasonable** behavior vis-a-vis information technologies
- Cybersecurity inconsistency with a **libertarian**, fluid and uncontrolled world.
- Need to establish core principles of **ethics, responsibility and transparency**
- Enshrining values in an appropriate **legal framework**; national/community-based/international
- Bringing into force **realistic rules** that are not only applicable locally but also applicable by the International Community and consistent with the existing international guidelines.

• PROBLEMS

- Emergence of **new forms of computer delinquency** where computers are used as **means** of classical offenses; for criminal **purposes** as they attack information systems; as criminal **tools** to commit sexual abuse on the minors, press and racial offences etc.
- Lack of an adequate **institutional framework** to address offences
- Absence of **criminal liability** for corporate bodies
- Risk of pirating copyrighted products
- Risk of offence to **human rights** in the process of individual data collection and processing
- **Informational unbalance** between individuals and companies, and administrations in charge of informationn

- SOLUTIONS

- ➔ Criminalizing and penalizing:

- Illegal access to an information system
- Infringement of confidentiality, availability of data and information systems
- Computer crimes
- Infringements relating to contents

• SOLUTIONS

- ➡ Putting sanction on corporate liability
- ➡ Setting restrictions to the rights people responsible for processing during the collection, use and transmission personal data
- ➡ Establishing new principles and rights to ensure transparency in the processing of information collected
- ➡ Protection of intellectual property rights against offences

PROBLEMS

- Inconsistency of criminal procedure rules with the search of evidence, computerization of data and telematics
- Risk of basic rights infringement in efforts toward effective investigations

SOLUTIONS

- Updating criminal procedures with regard to NICTs
- Setting up an consultation system evidence research in computer systems and creating a center of expertise and cybercrime control (by decree)
- Mainstreaming effective investigation requirements with the respect of basic rights.
- Developing judicial and police cooperation between regulatory authorities.
- Adhering to the convention of the European Council on Cybercrime.

- Setting up consultative and monitoring bodies for strategic prospective on cybersecurity
- Establishing an independent administrative authority to guarantee the respect of the principles and rights adopted
- Setting up:
 - reliable e-business infrastructures (accreditation, certification, standardization)
 - **legal and police jurisdictions** in the area of new technologies, with ability to cooperate with their colleagues from other countries;
 - Establishing a center of expertise on cybercrime.



THANKS FOR YOUR ATTENTION !

Abdoullah CISSE
University Lecture
Business and Cyber Law Expert
For your comments mail to :
acissea@gmail.com