

## The Convention on Cybercrime: an opportunity for African countries

### *La Convention sur la cybercriminalité: une opportunité pour les pays de l'Afrique*

Cybercrime legislation and capacity building workshop (US DOJ), Cotonou, Benin, 9-11 June 2008

Alexander Seger  
Council of Europe,  
Strasbourg, France  
Tel +33-3-9021-4506  
[alexander.seger@coe.int](mailto:alexander.seger@coe.int)

1

## 1 Cybercrime – current challenges Cybercriminalité – les défis

### Vulnerability of societies

### Vulnerabilité des sociétés

- **Offences against the confidentiality, integrity and availability of computer data and systems**  
Infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques  
  
**Example: Malware (worms, trojans, spyware, bots and botnets), Spam, DDOS attacks**  
Codes et logiciels malicieux (les virus, les vers, les chevaux de Troie, les logiciels espions, les robots et les réseaux zombies), spam, les attaques en déni de service
- **Offenders increasingly organising for crime aimed at generating illicit profits** Les criminels s'organisent pour obtenir des profits économiques  
  
**Example: Phishing and other forms of ID theft and fraud etc** Phishing et d'autres types de vols d'identité et de fraude
- **Content-related offences** Infractions se rapportant au contenu  
  
**Example: Child pornography, xenophobia, racisms etc.** Pornographie enfantine, xénophobie, racisms
- **Infringements of copyright and related rights** Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes

### Security / Sécurité – Human rights / Droits de l'homme

2

2

## 2

## The criminal law response La réponse de droit pénal

- **Criminalise certain conduct ► substantive criminal law**  
Criminaliser certaines conduites ► droit pénal matériel
- **Give law enforcement/criminal justice the means to investigate, prosecute and adjudicate cybercrimes (immediate actions, electronic evidence) ► criminal procedure law**  
Donner aux forces de l'ordre/à la justice pénale les moyens d'enquêter, de poursuivre et de juger les cyber crimes (actions immédiates, preuve électronique) ► code de procédure pénale
- **Allow for efficient international cooperation ► harmonise legislation, make provisions and establish institutions for police and judicial cooperation, conclude or join agreements**  
Permettre la coopération internationale efficace ► harmoniser la législation, faire des provisions et établir des institutions pour la coopération policière et juridique, conclure ou prendre part à des accords

3

## 3

## The Convention on Cybercrime La Convention sur la cybercriminalité

- **Elaborated by the Council of Europe with the participation of Canada, Japan, South Africa and the USA**  
Elaboré par le Conseil de l'Europe avec la participation du Canada, Japon, l'Afrique du Sud et les Etats-Unis
- **Opened for signature in Budapest in November 2001 Ouverte pour signature à Budapest, Novembre 2001**
- **In force since July 2004 En vigueur depuis juillet 2004**

## The Protocol on Xenophobia and Racism Committed through Computer Systems Protocole sur la xénophobie et le racisme par le biais de systèmes informatiques

- **Opened for signature in January 2003**
- **In force since March 2006**

4

4

## **Structure and content of the Convention** **Structure et contenu de la Convention**

**Chapter I: Definitions** (computer system/ système informatique, computer data/ données informatiques, service provider/ fournisseur de services, traffic data/ données relatives au trafic)

**Chapter II: Measures at national level** Mesures à prendre au niveau national

**Section 1 - Substantive criminal law (offences to be criminalised)** Droit pénal matériel

**Section 2 - Procedural law** Droit procédural

**Section 3 – Jurisdiction** Compétence

**Chapter III: International cooperation** Coopération internationale

**Section 1 - General principles** Principes généraux

**Section 2 - Specific provisions** Dispositions spécifiques

**Chapter IV: Final provisions** Clauses finales

5

5

## **Chapter II – Measures at national level** **Mesures à prendre au niveau national**

### **Section 1 – Substantive criminal law** Droit pénal matériel

- **Title 1 - Offences against the confidentiality, integrity and availability of computer data and systems (illegal access, illegal interception, data interference, system interference, misuse of devices)**

**Infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques (Accès illégal, Interception illégale, Atteinte à l'intégrité des données, Atteinte à l'intégrité du système, Abus de dispositifs)**

6

6

## Section 1 – Substantive criminal law

### Droit pénal matériel

- **Title 2 – Computer-related offences (forgery, fraud)** Infractions informatiques (Falsification, fraude)
- **Title 3 – Content-related offences (child pornography)** Infractions se rapportant au contenu (pornographie enfantine)
- **Title 4 – Infringements of copyright and related rights** Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes
- **Title 5 – Ancillary liability and sanctions (attempt, aiding, abetting, corporate liability, sanctions and measures)** Autres formes de responsabilité et de sanctions (Tentative et complicité, Responsabilité des personnes morales, Sanctions et mesures)

7

## Section 2 – Procedural law

### Droit procédural

- **Title 1 – Common provisions (scope of procedural provisions, conditions and safeguards)** Dispositions communes (Portée d'application des mesures du droit de procédure, Conditions et sauvegardes)
- **Title 2 – Expedited preservation of stored computer data (and traffic data and partial disclosure)** Conservation rapide de données informatiques stockées (de données informatiques stockées, divulgation partielle rapides de données relatives au trafic)
- **Title 3 – Production order** Injonction de produire
- **Title 4 – Search and seizure of stored computer data** Perquisition et saisie de données informatiques stockées
- **Title 5 – Real-time collection of computer data (traffic data, interception of content data)** Collecte en temps réel des données relatives au trafic (de données relatives au contenu)

*These apply to all criminal offences involving a computer system!*

8

## Chapter III - International cooperation

### Coopération internationale

#### Section 1 – General principles Principes généraux

- **Art 23 General principles on international cooperation** Principes généraux relatifs à la coopération internationale
- **Art 24 Principles related to extradition**
- **Art 25 Principles related to mutual legal assistance** Principes généraux relatifs à l'entraide
- **Art 26 Spontaneous information** Information spontanée
- **Art 27 MLA in the absence of applicable international instruments** Procédures relatives aux demandes d'entraide en l'absence d'accords internationaux applicables
- **Art 28 Confidentiality and limitation on use** Confidentialité et restriction d'utilisation

9

## Chapter III - International cooperation...

#### Section 2 – Specific provisions Dispositions spécifiques

- **Art 29 - Expedited preservation of stored computer data**  
Conservation rapide de données informatiques stockées
- **Art 30 - Expedited disclosure of preserved computer data**  
Divulgateion rapide de données conservées
- **Art 31 - Mutual assistance re accessing stored computer data**  
Entraide concernant l'accès aux données stockées
- **Art 32 - Trans-border access to stored computer data (public/with consent)** Accès transfrontière à des données stockées, avec consentement ou lorsqu'elles sont accessibles au public
- **Art 33 - Mutual assistance in real-time collection of traffic data**  
Entraide dans la collecte en temps réel de données relatives au trafic
- **Art 34 - Mutual assistance re interception of content data** Entraide en matière d'interception de données relatives au contenu
- **Art 35 - 24/7 network** Réseau 24/7

10

## Chapter IV – Final provisions **Clauses finales**

- **Art 36 Signature and entry into force (open to member States and non-members which have participated in its elaboration)**  
**Signature et entrée en vigueur**
- **Art 37 Accession**
- **Art 40 – 43 Declarations, reservations**
- **Art 46 – Consultations of the parties Concertation des Parties**

11

11

## **Implementation – current status** **Mise en oeuvre – état actuel**

- **The Convention entered into force in July 2004** **La Convention est entrée en vigueur en juillet 2004**
- **22 ratifications + 23 signatures (as of 1 July 2008)** **22 ratifications + 23 signatures (à la date du 1er juillet 2008)**
- **Signed by Canada, Japan, South Africa, ratified by USA** **Signée par le Canada, le Japon, l’Afrique du Sud et ratifiée par les Etats-Unis**
- **Costa Rica, Mexico, Philippines have been invited to accede**  
**Le Costa Rica, le Mexique et les Philippines ont été invités à accéder**
- **Legislative amendments underway in many other countries (Argentina, Brazil, Colombia, Egypt, India, Philippines etc.) and accession to the Convention under consideration** **Amendements législatifs en cours dans de nombreux autres pays (l’Argentine, le Brésil, la Colombie, l’Egypte, l’Inde, les Philippines etc...) et accession à la Convention en considération**
- = **Convention provides a global standard** **La Convention fournit un cadre normatif global**

12

**4****Accession to the Convention - benefits for countries of Africa**  
**Accession à la Convention – avantages pour les pays d’Afrique**

- **Coherent national approach to legislation on cybercrime**  
Approche nationale cohérente de la législation sur la cybercriminalité
- **Facilitates the gathering of electronic evidence**  
Faciliter le rassemblement des preuves électroniques
- **Facilitates the investigation of cyberlaundering, cyberterrorism and other serious crime**  
Faciliter les enquêtes sur le cyberblanchiment, le cyberterrorisme et autres crimes sérieux
- **Harmonisation and compatibility of criminal law provisions on cybercrime with those of other countries**  
Harmonisation et compatibilité des dispositions du code de procédure pénal sur le cybercrime avec ceux d’autres pays

13

**Accession to the Convention – benefits for countries of Africa**  
**Accession à la Convention – avantages pour les pays d’Afrique**

- **Legal and institutional basis for international law enforcement and judicial cooperation with other parties to the Convention**  
Base légale et institutionnelle pour la coopération internationale policière et juridique entre les Parties de la Convention
- **Participation in the Consultations of the Parties**  
Participation dans les Concertation des Parties
- **The treaty as a platform facilitating public-private cooperation**  
Le traité est une plate-forme facilitant la coopération entre le secteur public et le secteur privé

14

## How to accede to the Convention? Comment accéder à la Convention?

**Article 37: Convention is open for accession by third countries**  
**Article 37: La convention est ouverte à l'accession par les pays tiers**

**Accession process Processus d'accession :**

1. **Work on national legislation Préparer la législation nationale**
2. **Once legislation has been adopted or is in advanced stage, government to send a letter to Secretary General of CoE with a request to initiate consultation with parties to the Convention Une fois la législation adoptée ou à un état avancée, le gouvernement envoie un courrier au Secrétaire Général du Conseil de l'Europe avec une demande pour lancer la consultation des parties à la Convention**
3. **Secretariat of CoE will carry out consultations and put question before Committee of Ministers Le secrétariat du Conseil de l'Europe effectuera les consultations et posera la question au Comité des Ministres**
4. **After a positive vote, the country will be invited to accede Après un vote positif le pays sera invité à accéder**
5. **The country is then free to decide when to accede, that is, deposit the instrument of accession Le pays est alors libre de décider quand accéder, à savoir déposer l'instrument d'accession**

15

## 5 Model law function of the Convention La Convention comme une loi modèle

- **Use as / utiliser comme "checklist"**
- **Compare provisions comparer les articles**

**See country profiles on  
Voir profiles des pays sur**

[www.coe.int/cybercrime](http://www.coe.int/cybercrime)

Provision of / articles de la Convention	Provision in national law Disposition dans la législation nationale
Art 4 System interference Atteinte à l'intégrité du système	?
Art 6 Misuse of devices Abus de dispositifs	?
Art 9 Child pornography Pornographie infantine	?
Art 16 Expedited preservation Conservation rapide	?

16

## **Model law: example data interference**

### **Atteinte à l'intégrité des données**

#### Article 4 of the Convention: data interference

- Establish as criminal offences under domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

#### Article 4 – Atteinte à l'intégrité des données

- Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait, intentionnel et sans droit, d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques.

17

17

## **Example data interference**

### **Atteinte à l'intégrité des données**

#### In Romania / en Roumanie

##### ART.44 of Romania Law no 161/2003

(1) The alteration, deletion or deterioration of computer data or restriction to such data without right is a criminal offence and is punished with imprisonment from 2 to 7 years.

(2) The unauthorised data transfer from a computer system is punished with imprisonment from 3 to 12 years.

...

(1) Le fait de modifier, effacer ou détériorer des données informatiques ou de limiter l'accès à ces données, sans droit, représente une infraction et se punit par réclusion de 2 à 7 années.

(2) Le transfert non autorisé des données d'un système informatique se punit par réclusion de 3 à 12 années.

....

18

18

## **Example data interference**

### **Atteinte à l'intégrité des données**

FRANCE CODE PENAL

CHAPITRE III : Des atteintes aux systèmes de traitement automatisé de données

#### Article 323-1

Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30000 euros d'amende.

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45000 euros d'amende.

#### Article 323-3

Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75000 euros d'amende.

19

19

## **Model law: example expedited preservation**

### **Conservation rapide de données informatiques stockées**

#### **Article 16 of the Convention: Expedited preservation of stored computer data**

- 1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly **obtain the expeditious preservation of specified computer data, including traffic data**, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.

#### **Article 16 Conservation rapide de données informatiques stockées**

- 1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour permettre à ses autorités compétentes d'ordonner ou d'imposer d'une autre manière la conservation rapide de données électroniques spécifiées, y compris des données relatives au trafic, stockées au moyen d'un système informatique, notamment lorsqu'il y a des raisons de penser que celles-ci sont particulièrement susceptibles de perte ou de modification.

20

20

## **Example expedited preservation Conservation rapide de données informatiques stockées**

### **Expedited preservation of stored computer data under Romanian legislation**

**ART.54 of Romania Law no 161/2003**

- In urgent and duly justified cases, if there are data or substantiated indications regarding the preparation or the committing of a criminal offence by means of computer systems, in order to gather evidence or identify the perpetrators, it can be ordered the expeditious preservation of the computer data or traffic data, which are subject to the danger of destruction or alteration.
- The preservation is ordered by the prosecutor through a motivated ordinance, at the request of the criminal investigation body or ex-officio, and during the trial, by the court order.

21

21

## **Example expedited preservation Conservation rapide de données informatiques stockées**

**France** CODE DE PROCEDURE PENALE

**Article 60-2**

Sur demande de l'officier de police judiciaire, intervenant par voie télématique ou informatique, les organismes publics ou les personnes morales de droit privé ..... mettent à sa disposition les informations utiles à la manifestation de la vérité, à l'exception de celles protégées par un secret prévu par la loi, contenues dans le ou les systèmes informatiques ou traitements de données nominatives qu'ils administrent.

L'officier de police judiciaire, intervenant sur réquisition du procureur de la République préalablement autorisé par ordonnance du juge des libertés et de la détention, peut requérir des opérateurs de télécommunications ..... de prendre, sans délai, toutes mesures propres à assurer la préservation, pour une durée ne pouvant excéder un an, du contenu des informations consultées par les personnes utilisatrices des services fournis par les opérateurs.

22

22

**6****Providing support: The Project on Cybercrime  
Fournir d'assistance: le projet contre la  
cybercriminalité****Objective :**

To promote broad implementation of the  
Convention on Cybercrime (ETS 185) and its  
Protocol on Xenophobia and Racism (ETS 189)  
Promouvoir la mise en en oeuvre de la convention  
sur la cybercriminalité et du protocole sur la  
xénophobie et le racisme

1. Legislation
2. Training Formation
3. International cooperation Coopération  
internationale

**Duration Durée:**  
Sep 06 – Feb 09

**Funding  
Financement:**

➤ CoE, Microsoft,  
Estonia

**Phase 2:**

**Mar 2009 –  
Jun 2011**

23

**7****The way ahead Le chemin à parcourir**

- **Review legislation against the provisions of the Convention**  
Revoir la législation contre les dispositions de la  
Convention
- **If necessary take steps to strengthen legislation**  
Si nécessaire, prendre des mesures pour renforcer la  
législation
- **Consider accession to the Convention as a framework for  
international cooperation** Considérer l'accèsion à la  
Convention comme base de coopération internationale
- **Council of Europe ready to provide support: legislative  
analysis, workshops on cybercrime legislation** Le  
Conseil de l'Europe est prêt à fournir un soutien : analyse  
législative, ateliers sur la législation de cybercriminalité

24

24



[www.coe.int/cybercrime](http://www.coe.int/cybercrime)

**Thank you**

**Merci de votre attention**

**Alexander.seger@coe.int**