COUNCIL OF EUROPE CONSEIL DE L'EUROPE

www.coe.int/cybercrime

La Convention sur la cybercriminalité: une opportunité pour le Maroc

Rabat, juillet 2009

Alexander Seger
Council of Europe,
Strasbourg, France
Tel +33-3-9021-4506
alexander.seger@coe.int

1 Cybercriminalité – les defis

Dependance et vulnerabilité des sociétés

- Infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques
  Example: 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
- Les criminels s'organisent pour obtenir des profits economiques
  Example: Phishing et d'autres types de vols d'identité et de fraude
- Infractions se rapportant au contenu
  Example: Pornographie enfantine, xénophobie, racisms
- Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes
- Preuves électroniques

Securité – Droits de l'homme

2 La réponse de droit pénal

Criminaliser certaines conduites ▶ droit pénal matériel

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

Permettre la coopération internationale efficace ▶ harmoniser la légis-lation, faire des provisions et établir des institutions pour la coopération policière et juridique, conclure ou prendre part à des accords

3 La Convention sur la cybercriminalité

- Elaboré par le Conseil de l'Europe avec la participation du Canada, Japon, l'Afrique du Sud et les Etats-Unis
- Ouverte pour signature à Budapest, novembre 2001
- En vigeur dépuis juillet 2004

Protocol sur la xénophobie et le racisme par le biais de systèmes informatiques

- Ouvert pour signature en janvier 2003
- En vigeur dépuis mars 2006

Structure et contenu de la Convention

Chapitre I: Definitions (système informatique, données informatiques, fournisseur de services, données relatives au trafic)

Chapitre II: Mesures à prendre au niveau national
- Section 1 - Droit pénal matériel
- Section 2 - Droit procédural
- Section 3 - Compétence

Chapitre III: Coopération internationale
- Section 1 - Principes généraux
- Section 2 - Dispositions spécifiques

Chapitre IV: Clauses finales

Chapitre I – Mesures à prendre au niveau national

Section 1 – Droit pénal matériel

- Titre 1 - 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

Section 1 – Droit pénal matériel

- Titre 2 – Infractions informatiques (Falsification, fraude)
- Titre 3 – Infractions se rapportant au contenu (pornographie enfantine)
- Titre 4 – Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes
- Titre 5 – Autres formes de responsabilité et de sanctions (Tentative et complicité, Responsabilité des personnes morales, Sanctions et mesures)

7

Section 2 – Droit procédural

- Titre 1 – Dispositions communes (Portée d'application des mesures du droit de procédure, Conditions et sauvegardes)
- Titre 2 – Conservation rapide de données informatiques stockées (de données informatiques stockées, divulgation partielle rapides de données relatives au trafic)
- Titre 3 – Injonction de produire
- Titre 4 – Perquisition et saisie de données informatiques stockées
- Titre 5 – Collecte en temps réel des données relatives au trafic (de données relatives au contenu)

Chapitre III – Coopération internationale
Section 1 – Principes généraux

- Art 23 Principes généraux relatifs à la coopération internationale
- Art 24 Principes relatifs à extradition
- Art 25 Principes relatifs à l'entraide
- Art 26 Information spontanée
- Art 27 Procédures relatives aux demandes d'entraide en l'absence d'accords internationaux applicables
- Art 28 Confidentialité et restriction d'utilisation

Chapter III – Coopération internationale...
Section 2 – Dispositions spécifiques

- Art 29 - Conservation rapide de données informatiques stockées
- Art 30 - Divulgation rapide de données conservées
- Art 31 - Entraide concernant l'accès aux données stockées
- Art 32 - Accès transfrontière à des données stockées, avec consentement ou lorsqu'elles sont accessibles au public
- Art 33 - Entraide dans la collecte en temps réel de données relatives au trafic
- Art 34 - Entraide en matière d'interception de données relatives au contenu
- Art 35 - Réseau 24/7

Chapter IV – Clauses finales

- Art 36 – Signature et entrée en vigueur
- Art 37 – Accession
- Art 40 – 43 Declarations, reservations
- Art 46 – Concertation des Parties

11

Mise en oeuvre – état actuel

- La Convention est entrée en vigueur en juillet 2004
- 26 ratifications + 20 signatures (à la date du 1er juillet 2009)
- Signée par le Canada, le Japon, l'Afrique du Sud et ratifiée par les Etats-Unis
- Le Chili, le Costa Rica, la Republique Dominicaine, le Mexique et les Philippines ont été invités à accéder
- Amendements législatifs en cours dans de nombreaux autres pays (l'Argentine, le Brésil, la Colombie, l'Egypte, l'Inde, les Philippines etc…) et accession à la Convention en considération

= La Convention fournit un cadre normatif global

4 Accession à la Convention – avantages pour le Maroc

- Approche nationale cohérente de la législation sur la cybercriminalité
- Faciliter le rassemblement des preuves électroniques
- Faciliter les enquêtes sur le cyberblanchiment, le cyberterrorisme et autres crimes sérieux
- Harmonisation et compatibilité des dispositions du code de procédure pénal sur le cybercrime avec ceux d'autres pays
- Base légale et institutionnelle pour la coopération internationale policière et juridique entre les Parties de la Convention
- Participation dans les Concertation des Parties
- Le traité est une plate-forme facilitant la coopération entre le secteur public et le secteur privé

Comment accéder à la Convention?

Article 37: La convention est ouverte à l'accession par les pays tiers

Processus d'accession :

1. Préparer la legislation nationale
2. Une fois la législation adoptée ou à un état avancée, le gouvernement envoie un courrier au Secretaire Général du Conseil de l'Europe avec une demande pour lancer la consultation des parties à la Convention
3. Le secrétariat du Conseil de l'Europe effectuera les consultations et posera la question au Comité des Ministres
4. Après un vote positif le pays sera invité à accéder
5. Le pays est alors libre de décider quand accéder, à savoir déposer l'instrument d'accession

5 La Convention comme une loi modèle

- Utiliser comme "checklist"
- Comparer les articles

Voir profiles des pays sur

www.coe.int/cybercrime

Articles de la Convention	Disposition dans la legislation nationale
Art 4 Atteinte à l'intégrité du système	?
Art 6 Abus de dispositifs	?
Art 9 Pornographie infantine	?
Art 16 Conservation rapide	?

Loi modèle – Example: atteinte à l'intégrité des données

Convention 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.

En Roumanie Art.44 of Romania Law no 161/2003

(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.
....

16

Loi modèle – Example: 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.

17

Loi modèle – Example: Conservation rapide de données informatiques stockées

Convention 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.

18

Loi modèle – Example: 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.

19

Loi modèle – Example: 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.

20

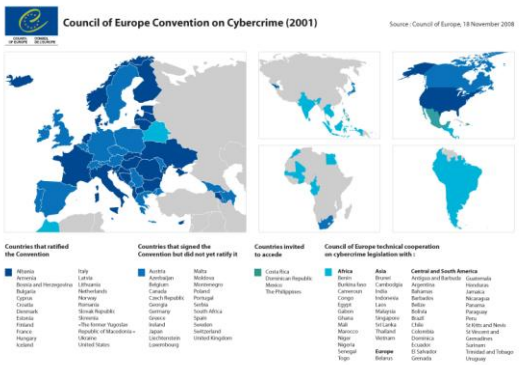
6 Fournir d'assistance: le projet contre la cybercriminalité

Objective :

Promouvoir la mise en en oeuvre de la convention sur la cybercriminalité et du protocol sur la xénophobie et le racisme

Phase 1: Sep 06 – Feb 09

Phase 2: Mar 2009 – Jun 2011



7 Le chemin à parcourir

- Revoir la législation contre les dispositions de la Convention
- Si nécessaire, prendre des mesures pour renforcer la législation
- Considérer l'accession à la Convention comme base de coopération internationale
- Le Conseil de l'Europe est prêt à fournir un soutien : analyse législative, ateliers sur la législation de cybercriminalité

23

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

www.coe.int/cybercrime

Merci de votre attention

Alexander.seger@coe.int

24