5 April 2019, Cotonou, Bénin
Organisé dans le cadre d'une visite du T-CY

Atelier d'information sur la

Convention de Budapest sur la Cybercriminalité

1. La Convention de Budapest: présentation
2. Cybercriminalité et preuves électroniques – les défis actuels et réponses du Bénin
3. Examen de la législation nationale sur la cybercriminalité par rapport aux dispositions de la Convention de Budapest
4. Conclusions : la voie à suivre pour le Bénin

www.coe.int/cybercrime

1

5 April 2019, Cotonou, Bénin
Organisé dans le cadre d'une visite du T-CY

Atelier d'information sur la

Convention de Budapest sur la Cybercriminalité

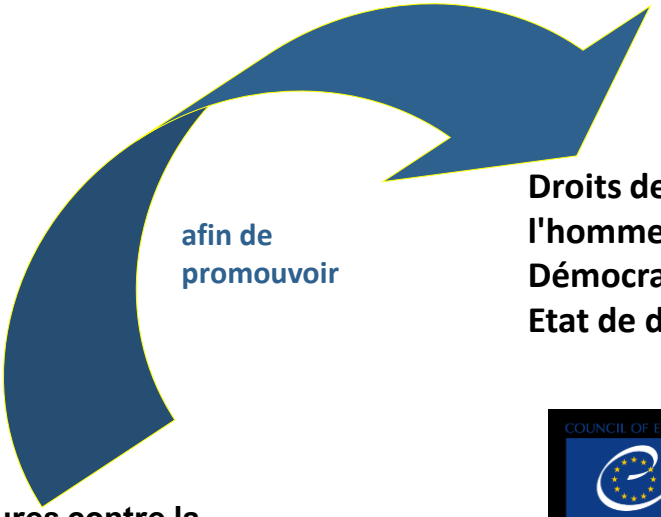
1. La Convention de Budapest: présentation

2. Cybercriminalité et preuves électroniques – les défis actuels et réponses du Bénin
3. Examen de la législation nationale sur la cybercriminalité par rapport aux dispositions de la Convention de Budapest
4. Conclusions : la voie à suivre pour le Bénin

www.coe.int/cybercrime

2

Coopération contre la cybercriminalité: l'approche du Conseil de l'Europe

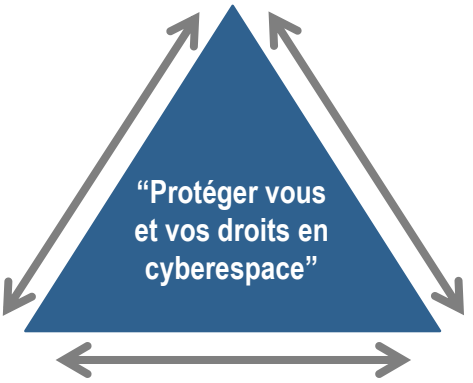


www.coe.int

3

Coopération contre la cybercriminalité: l'approche du Conseil de l'Europe

1 Standards communs : La Convention de Budapest sur la cybercriminalité et autres standards



2 Suivi: Cybercrime Convention Committee (T-CY)

3 Coopèration technique/ Capacity building ▶ C-PROC

4

La Convention de Budapest

- Ouverte pour signature à Budapest en novembre 2001
- Ouverte à l'adhésion par les pays tiers
- 63 Etats Parties + 8 Etats invites à adhérer
- Portée
  - Droit penal matériel
  - Droit procedural (cybercriminalité et preuves éléctronique)
  - Coopération internationale (cybercriminalité et preuves éléctronique)
- Suivi: Comité sur la cybercriminalité (T-CY)

5

La Convention de Budapest: procedure d'adhésion

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

Procédure d'adhésion:

1. Préparer la legislation nationale
2. Une fois la législation adoptée ou à un état avancée, et les capacité de coopérer disponible, le gouvernement envoie un courrier au Secrétaire Général du Conseil de l'Europe avec une demande de 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

6

La CoDnvention de Budapest: procedure d'adhésion

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

Procédure d'adhésion:

Déposer l'instrument d'accession

► **Obligatoire: Indiquer les autorités responsables pour**

- **Article 24 - Autorité responsable de l'envoi ou de la réception d'une demande d'extradition**
- **Article 27 – Autorités responsables pour l'entraide judiciaire**
- **Article 35 – Point de contact 24/7**

► **Si nécessaire: declarations et réserves**

7

La Convention de Budapest: portée

Droit pénal matériel

- Article 2 - Accès illégal
- Article 3 - Interception illégale
- Article 4 - Atteinte à l'intégrité des données
- Article 5 - Atteinte à l'intégrité du système
- Article 6 - Abus de dispositifs
- Article 7– Falsification informatique
- Article 8 – Fraude informatique
- Article 9 - Pornographie enfantine
- Article 10 - Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes

+

Droit procédural

- Article 14 – Portée d'application
- Article 15 – Conditions et sauvegardes
- Article 16 – Conservation rapide de données
- Article 17 – Conservation et divulgation rapides
- Article 18 – Injonction de produire
- Article 19 – Perquisition et saisie de données
- Article 20 – Collecte en temps réel des données relatives au trafic
- Article 21 – Interception de données relatives au contenu

+

Coopération internationale

Section 1 – Principes généraux (Articles 23 – 28)

Section 2 – Dispositions spécifiques (Articles 29 - 35)

- Art 29 - Conservation rapide
- Art 35 - Réseau 24/7

Harmonisation

8

À propos de la convention de Budapest

Portée

Cybercriminalité

- Infractions contre les systèmes informatiques et les données
- Infractions au moyen de systèmes informatiques et de données

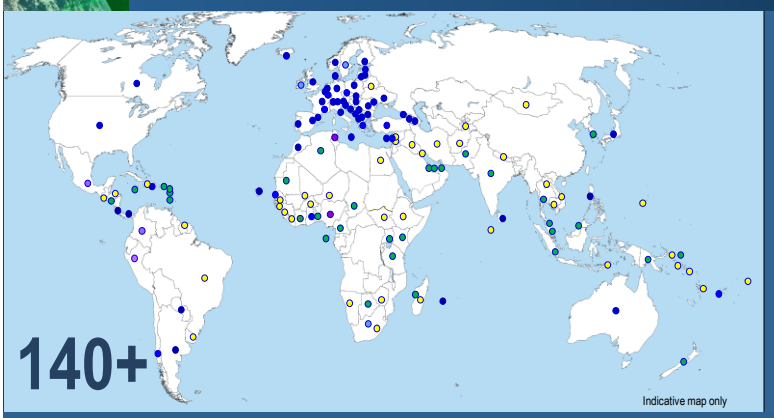
+

Preuve électronique

- Tout crime peut impliquer des preuves sous forme électronique sur un système informatique
- Nécessaire dans une procédure pénale
  Pas de données, pas de preuves, pas de justice

9

Etats faisants usage de la Convention de Budapest



Parties:

- ✓ Cabo Verde
- ✓ Ghana
- ✓ Mauritius
- ✓ Morocco
- ✓ Senegal

Signé / invite a adhéré:

- ○ Nigeria
- ○ South Africa
- ○ Tunésie

Ratific./adhésions: 63

Signé: 3

Invité a adhérer: 5

= 71

Etats avec (projets de) lois fondées sur la convention de Budapest = 20+

Autres états utilisant la convention = 50+

10

Maintenir à jour la Convention de Budapest

- **Protocole sur la xénophobie et le racisme via un ordinateur (31 Etats parties + 13 signataires)**
- **Notes d'orientation**
  - **Notion de systèmes informatiques**
  - **Botnets**
  - **Malware**
  - **Spam**
  - **Terrorisme**
  - **Accès transfrontalier aux données (Article 32)**
  - **Injonctions de produire des données relatives aux abonnés (Article 18)**
  - **Election interference [in preparation]**
- **Protocole sur la coopération internationale renforcée en cours de négociation**

= La Convention de Budapest reste à jour et pertinente

11

Les Conventions de Budapest et de Malabo

Echelle sous régionale: CEDEAO-Directive du 19 août 2011 relative à la lutte contre la cybercriminalité dans l'espace de la CEDEAO

La transposition par équivalence de la directive communautaire par le Bénin (Code du numérique)

Echelle continentale: Union africaine- Convention africaine de Malabo sur la cybersécurité et la protection des données à caractère personnel du 17 juin 2014

Exigence de la ratification de la Convention de Malabo

Echelle internationale: Convention de Budapest 2003

Faculté d'adhésion à la Convention (art. 35 de la Convention): premier instrument international de lutte contre la cybercriminalité

12

Analyse comparative des conventions de Budapest et de Malabo

- **Deux instruments de coopération différents**

Champ d'application:

- Convention de Budapest: instrument de justice pénale et de répression de la cybercriminalité (infractions pénale, instruments de procédure et techniques de coopération internationale)

- Convention de Malabo: instrument de cybersécurité qui couvre:
  - ✓ L'encadrement des transactions électroniques (chapitre 1er)
  - ✓ La protection des données à caractère personnel (chapitre II)
  - ✓ La promotion de la cybersécurité (chapitre III)
  - ✓ La lutte contre la cybercriminalité (chapitre III)

13

Analyse comparative des conventions de Budapest et de Malabo

- **Deux instruments de coopération différents**

Portée juridique:

- Convention de Budapest: instrument de coopération ouvert
- Possibilité d'adhésion par des Etats non membres du Conseil de l'Europe (USA, Canada, Cap Vert, Sénégal, Maurice, Japon, etc.) (art. 37)

- Convention de Malabo: instrument de coopération fermé:
- ouverte aux seuls Etats membres de l'Union africaine, « pour signature, ratification et adhésion, conformément à leurs procédures constitutionnelles respectives » (art. 35).

14

Analyse comparative des conventions de Budapest et de Malabo

- **Deux instruments de coopération différents**

Coopération judiciaire internationale:

- Convention de Budapest: prévision de mécanismes de coopération contre la cybercriminalité

✓ Les techniques de coopération aux fins d'investigation (perquisition transfrontalières, saisie de données, conservation rapide de données, etc.)
✓ informations spontanées
✓ le réseau 24/7;

- Convention de Malabo: Non prévision d'outils de coopération internationale
- Prévision d'une obligation pour les Etats de coopérer dans le cadre de la conclusion de conventions d'entraide judiciaire et d'échanges d'informations (article 28 paragraphe 2 de la Convention de Malabo)

15

Analyse comparative des conventions de Budapest et de Malabo

- **Deux instruments de coopération complémentaires**
  - La proximité des instruments de répression prévus par les deux conventions (infractions et pouvoirs de procédure)
  - La Convention de Budapest: une source d'inspiration de la Convention de Malabo
  - Convention de Malabo: le recours possible à d'autres instruments de coopération: les Etats parties s'engagent à se prévaloir des moyens existants pour la coopération internationale aux fins de répondre aux cybermenaces, à améliorer et à stimuler le dialogue entre les parties prenantes (article 29 paragraphe 4 de la Convention de Malabo)

16

Coopération contre la cybercriminalié: renforcer les capacités

1 Standards communs : La Convention de Budapest sur la cybercriminalité et autres standards

2 Suivi: Cybercrime Convention Committee (T-CY)

3 Coopèration technique/ Capacity building ▶ C-PROC

17

C-PROC tasks

Tâche: Soutien aux pays du monde entier pour renforcer les capacités de la justice pénale en matière de cybercriminalité et de preuve électronique

Sur la base de:

- Convention de Budapest sur la cybercriminalité
- Normes connexes, telles que
  - Protocole sur la xénophobie et le racisme via un ordinateur
  - Convention de Lanzarote sur la protection des enfants contre l'exploitation et les abus sexuels
  - Convention sur la protection des données 108 et protocoles
  - Convention sur le blanchiment de capitaux et le crime
- Exigences relatives aux droits de l'homme et à l'état de droit

18

C-PROC tasks

Projets gérés par C-PROC:

- **Renforcement de la législation sur la cybercriminalité et les preuves électroniques conformément aux normes de l'État de droit et des droits de l'homme (y compris la protection des données)**
- **Formation des juges, des procureurs et des agents de la force publique**
- **Mettre en place des unités spécialisées dans la cybercriminalité et la criminalistique et améliorer la coopération inter-institutions**
- **Promouvoir la coopération public / privé**
- **Protéger les enfants contre la violence sexuelle en ligne**
- **Renforcer l'efficacité de la coopération internationale**

19

C-PROC Programmes

30 personnes engagées dans 6 projets représentant un volume de 30 millions d'euros et couvrant toutes les régions du monde:

- **GLACY+** on Global Action on Cybercrime Extended (EU/COE Joint Project)
- **iPROCEEDS** Targeting proceeds from online crime in South-eastern Europe (EU/COE Joint Project)
- **Cybercrime@Octopus** resource for global capacity building (voluntary contribution funded)
- **CyberSouth** for the Southern Neighbourhood (EU/COE Joint Project)
- **EndOCSEA@Europe** on ending online child sexual exploitation and abuse (funded by WEPROTECT)
- **CyberEast** for the Eastern Partnership region (EU/COE Joint Project TBC)

20

Avantages de l'adhésion

- ✓ Reconnaissance d'un cadre juridique cohérent qui réponde aux exigences de l'état de droit
- ✓ Coopération fiable et efficace entre les Parties
- ✓ Participation au Comité de la Convention sur la cybercriminalité (T-CY)
- ✓ Participation à l'établissement de normes futures (protocoles et autres compléments à apporter à la Convention de Budapest)
- ✓ Confiance accrue par le secteur privé
- ✓ Assistance technique et renforcement des capacités

« Coût »: engagement à coopérer

Inconvénients: ?

21

5 April 2019, Cotonou, Bénin
Organisé dans le cadre d'une visite du T-CY

Atelier d'information sur la

Convention de Budapest sur la Cybercriminalité

1. La Convention de Budapest: présentation
2. **Cybercriminalité et preuves électroniques – les défis actuels et réponses du Bénin**
3. Examen de la législation nationale sur la cybercriminalité par rapport aux dispositions de la Convention de Budapest
4. Conclusions : la voie à suivre pour le Bénin

www.coe.int/cybercrime

22

Discussion:

- Quels sont les principaux défis pour le Bénin en matière de cybercriminalité et de preuve électronique?
- Avons-nous des données ou des statistiques sur la cybercriminalité?
- Quel est l'impact?

Discussion: Quelles sont les réponses du Bénin?

Législation?

- LOI N°2017 -20 DU 20 AVRIL 2018 PORTANT CODE DU NUMERIQUE EN REPUBLIQUE DU BENIN

Institutions, rôles, responsabilités?

- « Office Central de Répression de la Cybercriminalité [« OCRC »].

Défis?

Menaces

- Des centaines de millions d'incidents de vol de données personnelles chaque année
- Abus sexuel d'enfants en ligne
- Cyberintimidation, harcèlement et autres formes de cyberviolence
- Fraude massive générant des quantités massives de produits du crime
- Attaques contre des infrastructures d'informations critiques
- Ransomware
- Interférence dans les systèmes informatiques utilisés lors des élections
- Etc.

Menaces pour

- Droits de l'homme rights
- Démocracy
- Etat de droit
- Confiance et sécurité des TIC
- Développement économique

25

Cybercriminalité: Un problème d'état de droit et de la justice pénale

Cybercriminalité et autres infractions impliquant des preuves sur des systèmes informatiques (preuve électronique):

QUI L'A FAIT?

Pas de données, pas de preuves, pas de justice

- Des milliards d'utilisateurs et d'appareils
- Des milliards d'attaques
- Des millions d'infractions
- Existe-t-il un type de crime sans preuve électronique?
- Enquêtes%?
- Convictions%?

26

Où est la preuve?

- Cloud computing, territorialité et compétences
  - Cloud computing: systèmes distribués ▶ données distribuées ▶ preuves distribuées
  - Pas clair où les données sont stockées et / ou quel régime juridique s'applique
  - Fournisseur de service sous différentes juridictions
  - Ne sait pas quel fournisseur pour quels services contrôle quelles données
  - Les données sont-elles stockées ou en transit ▶ ordres de production, perquisition / saisie ou interception?

27

Cybercriminalité et preuve électronique:
Les défis de la justice pénale

Problèmes spécifiques à résoudre:

- Distinction des informations d'abonné par rapport aux données de trafic et de contenu
- Efficacité limitée de MLA
- Perte de localisation et jungle d'accès transfrontalier
- Fournisseur présent ou offrant un service sur le territoire d'une Partie
- Divulgation volontaire par les fournisseurs des États-Unis
- Procédures d'urgence
- Protection des données

28

Exemple: coopération volontaire par fournisseurs de service

	Requests for data directly sent to Apple, Facebook, Google, Microsoft, Twitter and Oath in 2017		
Parties and Observers (70 States)	Received	Disclosure	%
Albania	27	14	53%
Belgium	2 521	2 301	91%
Cabo Verde	40	20	50%
Croatia	196	166	85%
France	29 400	18 466	63%
Germany	35 596	20 172	57%
Mauritius	2	0	0%
Morocco	30	18	59%
Nigeria	7	5	71%
Portugal	3 569	2 394	67%
Senegal	2	0	0%
Turkey	8 618	4 739	55%
United Kingdom	31 954	23 073	72%
Total (excluding USA)	170 680	109 093	64%

29

Crime and jurisdiction in cyberspace
Crime et juridiction dans le cyberespace

► Solutions proposées dans le cadre de la Convention de Budapest

1. Solutions:
   Une MLA plus efficace
2. Note d'orientation sur l'article 18
3. Règles internes sur les ordres de production (article 18)
4. Coopération avec les fournisseurs: mesures pratiques
5. Protocole à la Convention de Budapest

30

Solution 5: Protocol

A. Dispositions pour une MLA plus efficace

- MLA accéléré pour l'information d'abonné
- Injonction a produire internationales
- Coopération directe entre les autorités judiciaires
- Enquêtes conjointes
- Procédures d'urgence pour l'accès aux données
- Rôle des points de contact 24/7

B. Dispositions relatives à la coopération directe avec les fournisseurs d'autres juridictions

C. Cadre et garanties pour les pratiques existantes d'accès transfrontière aux données

D. Sauvegardes / protection des données

Negotiations: Sep 2017 – 2020?

5 April 2019, Cotonou, Bénin
Organisé dans le cadre d'une visite du T-CY

Atelier d'information sur la

Convention de Budapest sur la Cybercriminalité

1. La Convention de Budapest: présentation
2. Cybercriminalité et preuves électroniques – les défis actuels et réponses du Bénin
3. **Examen de la législation nationale sur la cybercriminalité par rapport aux dispositions de la Convention de Budapest**
4. Conclusions : la voie à suivre pour le Bénin

Examen de la législation nationale: Droit pénal matériel

Convention de Budapest	Législation nationale
Article 2 – Accès illégal	Code du Numérique Article 507
Article 3 – Interception illégale	Article 508
Article 4 – Atteinte à l'intégrité des données	Article 510 + 508
Article 5 – Atteinte à l'intégrité du système	Article 509
Article 6 – Abus de dispositifs	Article 511
Article 7 – Falsification informatique	512
Article 8 – Fraude informatique	513
Article 9 – Infractions se rapportant à la pornographie enfantine	518
Article 10 – Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes	Chapitre VII Code du Numérique

33

Examen de la législation nationale: Définition des termes techniques

L'option de la définition des notions techniques

Convention de Budapest, art. 1er / Code du numérique, art. 1er

- Système informatique
- Données informatiques
- pornographie enfantine
- Mineur
- Données relatives aux abonnées
- Données relatives au trafic

Approche conceptuelle généralement conforme à la convention de Budapest.

34

Examen de la législation nationale: Droit pénal matériel

- **La création d'infractions nouvelles spécifiques aux TIC**
  - Les infractions relatives aux systèmes informatiques
  - Les infractions relatives aux données informatiques
  - Les infractions se rapportant à la pornographie enfantine
  - Les infractions informatiques
  - Les abus de dispositifs
  - Les infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes
  - Les actes racistes et xénophobes par le biais d'un système informatique

35

Examen de la législation nationale: Droit pénal matériel

Les infractions relatives aux données informatiques

- **Interception illégale de données informatiques** (art. 3 de la Convention)
  - Pénalisation de l'interception illégale (art. 508 du Code du numérique)
  - Circonstance aggravante: accès avec une intention frauduleuse (art. 508, al. 3 du Code du numérique)
  - Circonstance aggravante lorsque l'infraction est commise en rapport avec un système informatique connecté à un autre (art. 508, al 3 du Code du numérique)
- **Les atteintes à l'intégrité des données informatiques** (art. 4 de la Convention)
  - La pénalisation de l'effacement, l'endommagement, de la détérioration ou de l'altération de données (art.510 du Code du numérique)
  - Peines encourues même si les conséquences sur le système sont seulement temporaires ou permanentes (art. 510, al. 3 du Code du numérique).

36

Examen de la législation nationale: Droit pénal matériel

Les infractions se rapportant à la pornographie enfantine

- **La production en vue de sa diffusion, l'offre, la mise à disposition, la diffusion, la transmission de pornographie enfantine par le biais d'un système informatique** (art. 9 de la Convention)
  - Pénalisation des comportements (art. 518 du Code du numérique)
- **L'action de se procurer, de procurer à autrui, la possession de pornographie enfantine** (art. 9 de la Convention)
  - La pénalisation de l'acquisition, la détention ou la possession intentionnelle (art.518 du Code du numérique)

Les autres infractions relatives aux mineurs: inspirées de la Convention de Lanzerote et de la Convention africaine de Malabo

- Sollicitation de mineurs à des fins sexuelles (« grooming ») (art. 519 du Code du numérique)
- Consultation habituelle ou en contrepartie d'un paiement de la pornographie enfantine (art. 518 du Code du numérique)
- La facilitation de l'accès des mineurs à des contenus de pornographie (art . 520 du Code du numérique)

37

Examen de la législation nationale: Droit pénal matériel

Les infractions informatiques

- **La falsification informatique** (art. 7 de la Convention)
  - Pénalisation de la falsification informatique (art. 512 du Code du numérique)
  - Répression de l'usage des données informatiques falsifiées
- **La fraude informatique** (art. 8 de la Convention)
  - La transposition expresse de la Convention (art. 513 du Code du numérique)
- **Les abus de dispositifs** (art. 6 de la Convention)
  - Pénalisation de la production, de la vente, de l'importation, de l'exportation, de la diffusion d'un programme, donnée informatique principalement conçu ou adapté à la commission des infractions informatiques
  - Exemple: la diffusion d'un « Keylogger » (enregistreurs de frappe d'un clavier)

38

Examen de la législation nationale: Droit pénal matériel

Les infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes (art. 10 de la Convention)

- atteintes commises délibérément à une échelle commerciale;
- et au moyen d'un système informatique
- **Code du numérique: (art. 529-546)**

→ Complète les dispositions de la loi n° 2005-30 du 10 avril 2006 relative à la protection des droits d'auteurs et des droits voisins

- **La répression de la tentative et de la complicité des cyberinfractions** (art. 11 de la Convention)
- Sanction de la tentative et de la complicité (art. 580 et 581 du Code du numérique)

39

Examen de la législation nationale: Droit pénal matériel

La responsabilité pénale des personnes morales (art. 12 de la Convention)

- Encadrement (art. 494 du Code du numérique)
- Exclusion de la responsabilité pénale de l'Etat, des collectivités locales et des établissements publics
- Non exclusion de la responsabilité pénale de la personne physique auteur ou complice des faits
- Prévision des peines applicables aux personnes morales

Protocole additionnel sur le racisme et la xénophobie 2003

Code du Numérique
Article 552 : Incitation à la haine et à la violence
Article 556 : Négation, minimisation grossière, approbation ou justification d'un génocide ou de crimes contre l'humanité

40

Examen de la législation nationale: Droit pénal matériel

Code du Numérique:

Livre V – De la Protection des Données à caractère personnel

- **Convention sur la protection des données (Convention 108)**

41

Examen de la législation nationale: Droit pénal matériel

Convention de Budapest	Législation nationale
Article 2 – Accès illégal	Code du Numérique Article 507 ✓
Article 3 – Interception illégale	Article 508 ✓
Article 4 – Atteinte à l'intégrité des données	Article 510 + 508 ✓
Article 5 – Atteinte à l'intégrité du système	Article 509 ✓
Article 6 – Abus de dispositifs	Article 511 ✓
Article 7 – Falsification informatique	512 ✓
Article 8 – Fraude informatique	513 ✓
Article 9 – Infractions se rapportant à la pornographie enfantine	518 ✓
Article 10 – Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes	Chapitre VII Code Du Numérique ✓

42

Examen de la législation nationale: Droit pénal matériel

Convention de Budapest	Législation nationale
Article 11 – Tentative et complicité	Code du Numérique – Article 580 + 581✓
Article 12 – Responsabilité des personnes morales	Article 494 ✓

43

Examen de la législation nationale: Droit procédural

Convention de Budapest - Article 14 – Portée d'application des mesures du droit de procédure

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour instaurer les pouvoirs et procédures prévus dans la présente section aux fins d'enquêtes ou de procédures pénales spécifiques.

2 Sauf disposition contraire figurant à l'article 21, chaque Partie applique les pouvoirs et procédures mentionnés dans le paragraphe 1 du présent article:

a aux infractions pénales établies conformément aux articles 2 à 11 de la présente Convention;
b à toutes les autres infractions pénales commises au moyen d'un système informatique; et
c à la collecte des preuves électroniques de toute infraction pénale.

44

Examen de la législation nationale: Droit procédural

Code du Numérique - Article 492 : Champ d'application

Les pouvoirs et procédures prévus dans le présent Titre aux fins d'enquêtes ou de procédures pénales spécifiques s'appliquent :
1. aux infractions pénales établies conformément au Titre I du présent Livre ;
2. à toutes les autres infractions pénales commises sur et au moyen d'un système informatique ;
3. à la collecte des preuves électroniques de toute infraction pénale.

Article 577 : Mode de preuve électronique

L'écrit sous forme électronique, en application du Livre II, est, pour les besoins de l'application du présent Livre, admis en preuve au même titre que l'écrit sur support papier et possède la même force probante que celui-ci, sous réserve que puisse être dûment identifié la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité et la pérennité.

45

Examen de la législation nationale: Droit procédural

Convention de Budapest	Législation nationale
Article 16 – Conservation rapide de données informatiques stockées	Code du Numérique – Article 495 + 591
Article 17 – Conservation et divulgation rapides de données relatives au trafic	Article 592
Article 18 – Injonction de produire	Article 586
Article 19 – Perquisition et saisie de données informatiques stockées	Article 587 - 590
Article 20 – Collecte en temps réel des données relatives au trafic	Article 593
Article 21 – Interception de données relatives au contenu	Article 594
Article 22 – Compétence	Article 597

46

Examen de la législation nationale: Droit procédural

L'institution de nouveaux moyens d'investigation:

La convention article 16 la conservation rapide de données informatiques stockées

Pouvoir 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.

Code du numérique

Article 591 : Injonction de conserver et de protéger l'intégrité des données informatiques

Durée de conservation: 2 ans maximum

47

Examen de la législation nationale: Droit procédural

Convention de Budapest article 18 L'injonction de produire

Pouvoir d'ordonner:
a à une personne présente sur son territoire de communiquer les données informatiques spécifiées, en sa possession ou sous son contrôle, qui sont stockées dans un système informatique ou un support de stockage informatique; et
b à un fournisseur de services offrant des prestations sur le territoire de la Partie, de communiquer les données en sa possession ou sous son contrôle relatives aux abonnés et concernant de tels services.

Code du Numérique - Article 586 : Injonction de produire

Pouvoir d'ordonner à toute personne, tout établissement ou organisme privé ou public ou toute administration publique présentes sur le territoire ou fournissant des prestations de service en République du Bénin, susceptibles de détenir des documents intéressant l'enquête criminelle y compris ceux issus d'un système informatique ou un support de stockage informatique, de lui remettre ces documents, notamment sous forme numérique

48

Examen de la législation nationale: Droit procédural

Convention de Budapest article 21: L'interception de données relatives au contenu

- Pouvoir pour un éventail d'infractions graves de collecter ou d'enregistre ou d'obliger un fournisseur de services à collecter ou à enregistrer en temps réel les données relatives au contenu de communication transmises au moyen d'un système informatique :

Code du Numérique - article 594 : Interception et accès aux données par les autorités judiciaires

- Pouvoir du juge d'instruction de prescrire d'interception, l'enregistrement et la transmission de correspondances, y compris les données relatives au contenu émises par voie de communications électroniques

49

Examen de la législation nationale: Droit procédural

L'aménagement des outils classiques d'investigation:

Convention de Budapest: article 19 – Perquisition et saisie de données informatiques stockées

Le pouvoir des autorités compétentes à perquisitionner ou à accéder d'une façon similaire à un système informatique ou à une partie de celui-ci ainsi qu'aux données informatiques qui y sont stockées; et à un support du stockage informatique permettant de stocker des données informatiques sur son territoire.

Extension de la perquisition lorsque les données recherchées sont stockées dans un autre système informatique ou dans une partie de celui-ci situé sur son territoire, et que ces données sont légalement accessibles à partir du système initial ou disponibles pour ce système initial

50

50

Examen de la législation nationale: Droit procédural

Code du Numérique - Article 587 : Données stockées dans un système informatique

Pouvoir d'opérer une perquisition ou d'accéder à un système informatique ou à une partie de celui-ci ou dans un autre système informatique ou un support et aux données présentes dans ces derniers dès lors que ces données sont accessibles à partir du système initial ou disponible pour le système initial.

Perquisition transfrontalière: S'il est préalablement avéré que ces données, accessibles à partir du système initial ou disponible pour le système initial, sont stockées dans un autre système informatique situé en dehors du territoire national, elles sont recueillies par le juge d'instruction, par voie de commission rogatoire internationale.

Examen de la législation nationale: Droit procédural

Convention de Budapest: La saisie électronique (art. 19 3)

En cas de découverte de données utiles aux investigations: pouvoir de saisir ou d'obtenir de façon similaire, de réaliser une copie des données, de préserver l'intégrité des données informatique stockées et de rendre inaccessibles les données

Code du numérique: article 590 : Copie des données

En cas de découverte de données utiles aux investigations: pouvoir du juge d'instruction de copier les données sur des supports de stockage informatique pouvant être saisis et placés sous scellés.

Examen de la législation nationale: Droit procédural

Convention de Budapest Article 15 – Conditions et sauvegardes

Soumission des outils de procédure aux conditions et sauvegardes prévus par le droit interne et les instruments internationaux de protection des droits de l'Homme. en application de la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales du Conseil de l'Europe (1950) et du Pacte international relatif aux droits civils et politiques des Nations Unies (1966), ou d'autres instruments internationaux applicables concernant les droits de l'homme, et qui doit intégrer le principe de la proportionnalité.

Autres sauvegardes: l'existence d'une supervision judiciaire ou d'autres formes de supervision indépendante, des motifs justifiant l'application ainsi que la limitation du champ d'application et de la durée du pouvoir ou de la procédure.

53

Examen de la législation nationale: Droit procédural

Code du numérique Article 493 : Garantie des droits fondamentaux et des libertés

La soumission de la mise en œuvre des pouvoirs et procédures aux conditions et sauvegardes prévues par le droit interne de la République du Bénin, qui doit assurer une protection adéquate des droits de l'homme et des libertés, en particulier des droits établis conformément aux obligations que celle-ci a souscrites en application du Pacte international relatif aux droits civils et politiques des Nations-Unies et de la Charte africaine des droits de l'homme et des peuples ou d'autres instruments internationaux applicables concernant les droits de l'homme, et qui doit intégrer le principe de la proportionnalité.

Cas de d'application des sauvegardes:

- l'interception de données relatives au contenu prévue seulement en matière criminelle et en matière délictuelle si la peine encourue est au moins égale à 2 ans (principe de proportionnalité) (art. 594 du Code du numérique)
- L'existence d'une supervision judiciaire: compétence exclusive du juge d'instruction (art. 594 du Code du numérique)

54

Examen de la législation nationale: Droit procédural

Code Numérique

CHAPITRE II DE L'OFFICE CENTRAL DE REPRESSION DE LA CYBERCRIMINALITE

Article 608 : Organe de lutte contre la Cybercriminalité

La structure de lutte contre les infractions cybernétiques est dénommée « Office Central de Répression de la Cybercriminalité [« OCRC »].
L'OCRC, placé sous la tutelle du Ministère en charge de la sécurité publique, a une compétence nationale.
Sont associés aux activités de cet Office, le Ministère en charge de la défense nationale, le Ministère en charge des finances et le Ministère en charge des communications électroniques.

Article 609 : Compétences

L'OCRC a pour domaine de compétence, les infractions spécifiques à la criminalité liées aux technologies de l'information et de la communication.
Dans les conditions fixées à l'article suivant, sa compétence s'étend aux infractions dont la commission est facilitée ou liée à l'utilisation de ces technologies.

55

Examen de la législation nationale: Droit procédural

Code Numérique

Article 610 : Missions et attributions

L'OCRC a pour missions :

1. de veiller à la prise de mesures préventives contre la cybercriminalité ;
2. d'animer et de coordonner, au niveau national, la mise en oeuvre opérationnelle de la lutte contre les auteurs et complices d'infractions spécifiques à la criminalité liée aux technologies de l'information et de la communication ;
3. d'effectuer conformément au code de procédure pénale les enquêtes sur les infractions visant ou utilisant les systèmes informatiques ainsi que les modes de traitement, de stockage et de communication de l'information ;
4. d'apporter son concours technique aux autres services de sécurité à l'occasion des enquêtes en cours nécessitant ses compétences techniques ou son expertise ;
5. d'assurer en liaison avec les services compétents, les actions de formation et d'information visant à renforcer les capacités opérationnelles des agents de tous les services concourant à la lutte contre ce fléau ;
6. d'intervenir d'initiative, sous la direction de l'autorité judiciaire saisie, chaque fois que les circonstances l'exigent, pour s'informer sur place des faits relatifs aux investigations conduites

56

Examen de la législation nationale: Droit procédural

Code Numérique

Article 611 : Organisation de l'OCRC

La composition, l'organisation et les modalités de fonctionnement de l'OCRC sont précisés par décret pris en Conseil des Ministres.
Pour accomplir sa mission, l'OCRC centralise, analyse, exploite et communique aux services de la police nationale, de la gendarmerie nationale, de la direction générale des douanes et droits indirects ainsi qu'aux autres administrations et services publics de l'État concernés, toutes informations relatives aux faits et infractions liés aux technologies de l'information et de la communication. Il établit également les liaisons utiles avec les organismes du secteur privé concernés.

Article 612 : Transmission d'informations

Dans le cadre de la législation applicable, notamment en matière de secret professionnel, les services de la police nationale, de la gendarmerie nationale, de la direction générale des douanes et droits indirects ainsi que les autres administrations et services publics de l'Etat concernés, adressent, dans les meilleurs délais, à l'OCRC les informations relatives aux infractions visées au présent livre dont ils ont connaissance.

57

Examen de la législation nationale: Droit procédural

Code Numérique

Article 613 : Coopération

Pour les infractions relevant de sa compétence définie au 1er alinéa de l'article 609, l'OCRC constitue, pour la République du Bénin, le point de contact central dans les échanges internationaux. Il contribue au niveau national à l'animation et à la coordination des travaux préparatoires nécessaires et participe aux activités des organes et enceintes internationaux. Sans préjudice de l'application des conventions internationales, il entretient les liaisons opérationnelles avec les services spécialisés des autres pays et avec les organismes internationaux en vue de rechercher toute information relative aux infractions ainsi qu'à l'identification et à la localisation de leurs auteurs.

Article 614 : Collaboration

L'OCRC collabore avec toutes les administrations publiques ou privées qui sollicitent son assistance technique ou son expertise pour se mettre à l'abri des méfaits criminels.

58

Examen de la législation nationale: Droit procédural

Convention de Budapest	Législation nationale
Article 16 – Conservation rapide de données informatiques stockées	Code du Numérique – Article 495 + 591✓
Article 17 – Conservation et divulgation rapides de données relatives au trafic	Article 592 ✓
Article 18 – Injonction de produire	Article 586 ✓
Article 19 – Perquisition et saisie de données informatiques stockées	Article 587 – 590 ✓
Article 20 – Collecte en temps réel des données relatives au trafic	Article 593 ✓
Article 21 – Interception de données relatives au contenu	Article 594 ✓
Article 22 – Compétence	Article 597 ✓

59

Coopération Internationale

Convention de Budapest	
Article 23 – Principes généraux relatifs à la coopération internationale	
Article 24, 25, 26, 27	
Article 29 – Conservation rapide de données informatiques stockées	
Article 30 – Divulgation rapide de données conservées	
Article 31 – Entraide concernant l'accès aux données stockées	
Article 32 – Accès transfrontière à des données stockées, avec consentement ou lorsqu'elles sont accessibles au public	
Article 33 – Entraide dans la collecte en temps réel de données relatives au trafic	
Article 34 – Entraide en matière d'interception de données relatives au contenu	
Article 35 – Réseau 24/7	

60

Coopération Internationale

Quelles dispositions pour la coopération internationale?

61

Examen de la législation nationale: conclusion

- Droit matériel ✓
- Droit procedural ✓
- Coopération internationale **(si Partie a la Convention de Budapest)**

62

5 April 2019, Cotonou, Bénin
Organisé dans le cadre d'une visite du T-CY

Atelier d'information sur la

Convention de Budapest sur la Cybercriminalité

1. La Convention de Budapest: présentation
2. Cybercriminalité et preuves électroniques – les défis actuels et réponses du Bénin
3. Examen de la législation nationale sur la cybercriminalité par rapport aux dispositions de la Convention de Budapest
4. **Conclusions : la voie à suivre pour le Bénin**

www.coe.int/cybercrime

63

Conclusions

Discussion:

Quelle voie à suivre pour le Bénin?

64

65