12 mars 2019, Abidjan, Côte d'Ivoire
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 de la Côte d'Ivoire
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 la Côte d'Ivoire

www.coe.int/cybercrime

1

12 mars 2019, Abidjan, Côte d'Ivoire
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 de la Côte d'Ivoire
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 la Côte d'Ivoire

www.coe.int/cybercrime

2

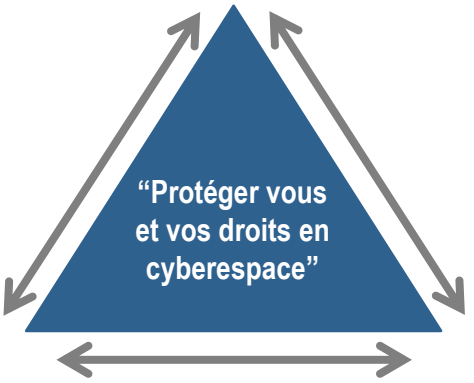
Coopération contre la cybercriminalité: l'approche du Conseil de l'Europe

COUNCIL OF EUROPE
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 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

7

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

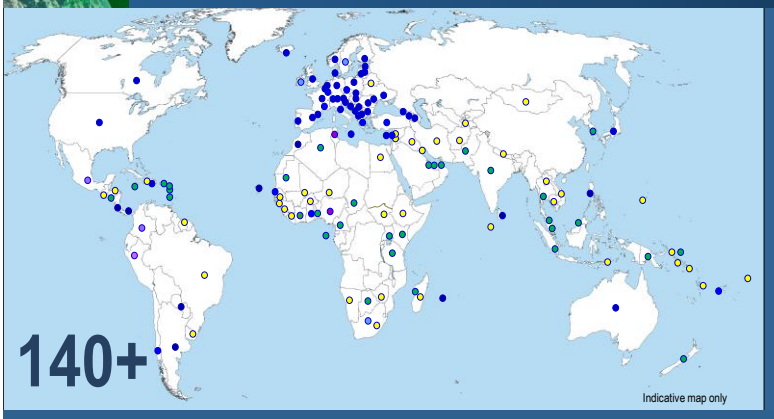
+

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

8

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+

9

Maintenir à jour la Convention de Budapest

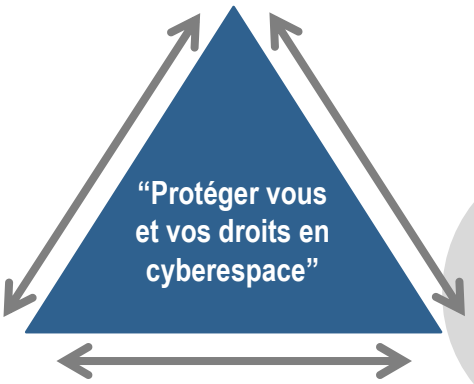
- ► Protocol on Xenophobia and Racisms via Computer Systems (31 Parties + 13 Signatories)
- ► Guidance Notes on
  - Notion of computer systems
  - Botnets
  - Malware
  - Spam
  - Terrorism
  - Transborder access to data (Article 32)
  - Production Orders for Subscriber Information (Article 18)
  - Election interference [in preparation]
- ► Protocole sur la coopération internationale renforcée en cours de négociation

= La Convention de Budapest reste à jour et pertinente

10

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

11

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

12

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**

13

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)

14

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: ?

15

12 mars 2019, Abidjan, Côte d'Ivoire
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 de la Côte d'Ivoire**
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 la Côte d'Ivoire

www.coe.int/cybercrime

16

Discussion:

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

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

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%?**

19

Cybercriminalité et preuve électronique: Les défis de la justice pénale

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?**

20

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

21

Example: voluntary cooperation by providers

	Requests for data sent to Apple, Facebook, Google, Microsoft, Twitter and Yahoo in 2015		
Parties	Received	Disclosure	%
Austria	254	119	47%
Belgium	1 992	1 453	73%
Canada	1 157	884	76%
France	27 213	14 746	54%
Germany	29 092	15 469	53%
Italy	7 847	3 591	46%
Netherlands	1 605	1 213	76%
Poland	2 378	820	34%
Portugal	3 255	1 751	54%
Spain	4 151	2 092	50%
United Kingdom	29 937	21 075	70%
USA	89 350	70 116	78%
Total excluding USA	**138 612**	**82 529**	**60%**
Total including USA	227 962	152 644	67%

22

► 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

23

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?

24

Discussion: Quelles sont les réponses de la Côte d'Ivoire?

Législation:

- **Loi n°2013-451 relative à la lutte contre la cybercriminalité**
- **Loi n°2013-450 relative à la protection des données à caractère personnel**
- **Loi n°2013-546 relative aux transactions électroniques**
- **Autres?**

Institutions, rôles, responsabilités?

Défis?

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 de la Côte d'Ivoire
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 la Côte d'Ivoire

Examen de la législation nationale: Droit pénal matériel

Convention de Budapest	Législation nationale
Article 2 – Accès illégal	Loi 2013-451 : article 4
Article 3 – Interception illégale	Article 8 et 31
Article 4 – Atteinte à l'intégrité des données	Article 9
Article 5 – Atteinte à l'intégrité du système	Article 6
Article 6 – Abus de dispositifs	Article 13 et 29
Article 7 – Falsification informatique	Article 10
Article 8 – Fraude informatique	Article 12
Article 9 – Infractions se rapportant à la pornographie enfantine	Article 15, 16, 17
Article 10 – Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes	Article 33 et 34

27

Examen de la législation nationale: Droit pénal matériel

Budapest Article 2 – Accès illégal

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'accès intentionnel et sans droit à tout ou partie d'un système informatique. Une Partie peut exiger que l'infraction soit commise en violation des mesures de sécurité, dans l'intention d'obtenir des données informatiques ou dans une autre intention délictueuse, ou soit en relation avec un système informatique connecté à un autre système informatique.

Loi 2013-451

Article 4: est puni de un à deux an d'emprisonnement et de 5.000.000 à 10.000.000 de francs CFA d'amende, quiconque accde ou tente d'accéder frauduleusement à tout ou partie d'un systèmd d'information.

28

Examen de la législation nationale: Droit pénal matériel

Budapest Article 3 – Interception illégale

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'interception intentionnelle et sans droit, effectuée par des moyens techniques, de données informatiques, lors de transmissions non publiques, à destination, en provenance ou à l'intérieur d'un système informatique, y compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données informatiques. Une Partie peut exiger que l'infraction soit commise dans une intention délictueuse ou soit en relation avec un système informatique connecté à un autre système informatique.

29

Examen de la législation nationale: Droit pénal matériel

Loi 2013-451

Article 8 : « Est puni de cinq à dix ans d'emprisonnement et de 40.000.000 à 60.000.000 de francs CFA d'amende, quiconque intercepte ou tente d'intercepter frauduleusement par des moyens techniques des données informatiques lors de leur transmission non publique à destination, en provenance ou à l'intérieur d'un système d'information ».

Article 31 : « Est puni d'un emprisonnement de un à cinq ans et de 1.000.000 de francs CFA d'amende, quiconque de mauvaise foi, ouvre, supprime, retarde ou détourne des correspondances électroniques arrivées ou non à destination et adressées à un tiers, ou en prend frauduleusement connaissance. Est puni des mêmes peines, quiconque de mauvaise foi, intercepte, détourne, utilise ou divulgue des correspondances électroniques émises, transmises ou reçues par la voie des télécommunications ou procède à l'installation d'appareils conçus pour réaliser de telles interceptions ».

30

Examen de la législation nationale: Droit pénal matériel

Budapest Article 4 – Atteinte à l'intégrité des données

1 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.

2 Une Partie peut se réserver le droit d'exiger que le comportement décrit au paragraphe 1 entraîne des dommages sérieux.

Loi 2013-451

Article 9 : « Est puni de cinq à dix ans d'emprisonnement et de 40.000.000 à 60.000.000 de francs CFA d'amende, quiconque altère ou tente d'altérer, modifie ou tente de modifier, supprime ou tente de supprimer frauduleusement des données informatiques ».

31

Examen de la législation nationale: Droit pénal matériel

Budapest Article 5 – Atteinte à l'intégrité du système

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'entrave grave, intentionnelle et sans droit, au fonctionnement d'un système informatique, par l'introduction, la transmission, l'endommagement, l'effacement, la détérioration, l'altération ou la suppression de données informatiques.

Loi 2013-451

Article 6 : « Est puni de un à cinq ans d'emprisonnement et de 10.000.000 à 40.000.000 de francs CFA d'amende, quiconque entrave, fausse ou tente d'entraver ou de fausser frauduleusement le fonctionnement d'un système d'information ».

Voir également, par extension, **l'article 30** qui dispose : « Lorsque les faits punis par la présente loi portent sur un système d'information ou un programme de traitement de données protégé par un code d'accès secret, la peine encourue ne peut être inférieure à dix ans d'emprisonnement ».

32

Examen de la législation nationale: Droit pénal matériel

Budapest Article 6 – Abus de dispositifs

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, lorsqu'elles sont commises intentionnellement et sans droit:

a la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition:

i d'un dispositif, y compris un programme informatique, principalement conçu ou adapté pour permettre la commission de l'une des infractions établies conformément aux articles 2 à 5 ci-dessus;
ii d'un mot de passe, d'un code d'accès ou de données informatiques similaires permettant d'accéder à tout ou partie d'un système informatique,
dans l'intention qu'ils soient utilisés afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5; et

b la possession d'un élément visé aux paragraphes a.i ou ii ci-dessus, dans l'intention qu'il soit utilisé afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5.

33

Examen de la législation nationale: Droit pénal matériel

Loi 2013-451

Article 13 :

« Est puni de un an à deux ans d'emprisonnement et de 10.000.000 à 50.000.000 de francs CFA d'amende, quiconque, dans l'intention de commettre l'une des infractions prévues par la présente loi produit, vend, importe, détient, diffuse, offre, cède ou met à disposition, en connaissance de cause :

- **un équipement, un dispositif ou un programme informatique**
- **un mot de passe, un code d'accès ou des données informatiques similaires ».**

34

Examen de la législation nationale: Droit pénal matériel

Loi 2013-451

Article 29 : « **Lorsqu'elle est faite intentionnellement et sans droit, la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition d'un dispositif, y compris un programme informatique, principalement conçu ou adapté pour permettre la commission d'un vol d'information, ou l'usage d'un mot de passe, d'un code d'accès ou de données informatiques similaires permettant d'accéder à tout ou partie d'un système d'information, dans l'intention qu'ils soient utilisés afin de commettre l'une ou l'autre des infractions prévues par de la présente loi, est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée d'entre elles».**

Voir également, par extension, l'article 30, précité.

35

Examen de la législation nationale: Droit pénal matériel

Budapest Article 8 – Fraude informatique

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 de causer un préjudice patrimonial à autrui:

a par toute introduction, altération, effacement ou suppression de données informatiques;

b par toute forme d'atteinte au fonctionnement d'un système informatique,

dans l'intention, frauduleuse ou délictueuse, d'obtenir sans droit un bénéfice économique pour soi-même ou pour autrui.

36

Examen de la législation nationale: Droit pénal matériel

Loi 2013-451

Article 12 : « Est puni de un à cinq ans d'emprisonnement et de 30.000.000 à 50.000.000 de francs CFA d'amende, quiconque obtient frauduleusement, pour soimême ou pour autrui, un avantage quelconque, par l'introduction, l'utilisation, la modification, l'altération ou la suppression de données informatiques ou par toute forme d'atteinte au système d'information ».

37

Examen de la législation nationale: Droit pénal matériel

Budapest Article 9 – Infractions se rapportant à la pornographie enfantine

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les comportements suivants lorsqu'ils sont commis intentionnellement et sans droit:

a la production de pornographie enfantine en vue de sa diffusion par le biais d'un système informatique;

b l'offre ou la mise à disposition de pornographie enfantine par le biais d'un système informatique;

c la diffusion ou la transmission de pornographie enfantine par le biais d'un système informatique;

d le fait de se procurer ou de procurer à autrui de la pornographie enfantine par le biais d'un système informatique;

e la possession de pornographie enfantine dans un système informatique ou un moyen de stockage de données informatiques.

38

Examen de la législation nationale: Droit pénal matériel

Budapest Article 9 – Infractions se rapportant à la pornographie enfantine

2 Aux fins du paragraphe 1 ci-dessus, le terme «pornographie enfantine» comprend toute matière pornographique représentant de manière visuelle:

a un mineur se livrant à un comportement sexuellement explicite;

b une personne qui apparaît comme un mineur se livrant à un comportement sexuellement explicite;

c des images réalistes représentant un mineur se livrant à un comportement sexuellement explicite.

3 Aux fins du paragraphe 2 ci-dessus, le terme «mineur» désigne toute personne âgée de moins de 18 ans. Une Partie peut toutefois exiger une limite d'âge inférieure, qui doit être au minimum de 16 ans.

39

Examen de la législation nationale: Droit pénal matériel

Loi 2013-451

Article 15 : « Est puni de deux à cinq ans d'emprisonnement et de 75.000.000 à 100.000.000 de francs CFA d'amende, quiconque produit, enregistre, offre, met à disposition, diffuse, transmet une image ou une représentation présentant un caractère de pornographie infantile par le biais d'un système d'information ou d'un moyen de stockage de données informatiques ».

Article 16 : « Est puni de deux à cinq ans d'emprisonnement et de 75.000.000 à 100.000.000 de francs CFA d'amende, quiconque se procure ou procure à autrui, importe ou fait importer, exporte ou fait exporter une image ou une représentation présentant un caractère de pornographie infantile par le biais d'un système d'information ou d'un moyen de stockage de données informatiques »..

Article 17 : « Est puni de un à trois ans d'emprisonnement et de 20.000.000 à 40.000.000 de francs CFA d'amende, quiconque possède intentionnellement une image ou une représentation présentant un caractère de pornographie infantile dans un système d'information ou dans un moyen de stockage de données informatiques ».

40

Examen de la législation nationale: Droit pénal matériel

Loi 2013-451

Article 1 , **pornographie infantile** : toute donnée quelle qu'en soit la nature ou la forme représentant de manière visuelle un enfant de moins de dix-huit ans se livrant à un agissement sexuellement explicite ou des images représentant un enfant de moins de quinze ans se livrant à un comportement sexuellement explicite ;

Article 1 , **mineur** : toute personne âgée de moins de dix-huit ans, conformément au code pénal ;

41

Examen de la législation nationale: Droit pénal matériel

Convention de Budapest	Législation nationale
Article 2 – Accès illégal	Loi 2013-451 : article 4 ✓
Article 3 – Interception illégale	Article 8 et 31 ✓
Article 4 – Atteinte à l'intégrité des données	Article 9 ✓
Article 5 – Atteinte à l'intégrité du système	Article 6 ✓
Article 6 – Abus de dispositifs	Article 13 et 29 ✓
Article 7 – Falsification informatique	Article 10 ✓
Article 8 – Fraude informatique	Article 12 ✓
Article 9 – Infractions se rapportant à la pornographie enfantine	Article 15, 16, et 17 ✓
Article 10 – Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes	Article 33 et 34 ✓

42

Examen de la législation nationale: Droit pénal matériel

Convention de Budapest	Législation nationale
Article 11 – Tentative et complicité	Loi 2013-451 Tentative: Articles 4, 5, 6 ✓ Complicité: Articles 28, 36, 69 ✓
Article 12 – Responsabilité des personnes morales	Article 69 ✓

43

Examen de la législation nationale: Droit procédural

Convention de Budapest	Législation nationale
Article 16 – Conservation rapide de données informatiques stockées	Loi 2013-451 Articles 73 et 78 ✓
Article 17 – Conservation et divulgation rapides de données relatives au trafic	Articles 73, 74 et 78
Article 18 – Injonction de produire	Articles 74 ✓
Article 19 – Perquisition et saisie de données informatiques stockées	Articles 71, 74 et 75 ✓
Article 20 – Collecte en temps réel des données relatives au trafic	Article 77 ✓
Article 21 – Interception de données relatives au contenu	Article 77 ✓
Article 22 – Compétence	Article 3 et 41 ✓

44

Examen de la législation nationale: Droit procédural

Convention de Budapest	Législation nationale
Article 16 – Conservation rapide de données informatiques stockées	Loi 2013-451 Articles 73 et 78
Article 17 – Conservation et divulgation rapides de données relatives au trafic	Articles 73, 74 et 78
Article 18 – Injonction de produire	Articles 74 et 77
Article 19 – Perquisition et saisie de données informatiques stockées	Articles 71, 74 et 75
Article 20 – Collecte en temps réel des données relatives au trafic	Article 77
Article 21 – Interception de données relatives au contenu	Article 77
Article 22 – Compétence	Article 3 et 41

45

Examen de la législation nationale: Droit procédural

Budapest 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.

….

46

Examen de la législation nationale: Droit procédural

Loi 2013-451

Article 73 : « Lorsque dans le cadre d'une enquête ou d'une instruction, il y a des raisons de penser que des données informatiques spécifiées, y compris des données relatives aux abonnés et au trafic, stockées au moyen d'un système d'information, sont susceptibles de perte ou de modification, l'autorité compétente procède ou fait procéder à la conservation immédiate desdites données.

La personne physique ou morale à qui injonction est faite, conserve et protège l'intégrité desdites données pendant une durée aussi longue que nécessaire pour les besoins de l'enquête ou de l'instruction ».

47

Examen de la législation nationale: Droit procédural

Convention de Budapest / Article 18 – Injonction de produire

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à 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.

2 Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

48

Examen de la législation nationale: Droit procédural

Convention de Budapest / Article 18 – Injonction de produire

…..

3 Aux fins du présent article, l'expression «données relatives aux abonnés» désigne toute information, sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de services et se rapportant aux abonnés de ses services, autres que des données relatives au trafic ou au contenu, et permettant d'établir:
a le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service;
b l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de services;
c toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de services.

49

Examen de la législation nationale: Droit procédural

Loi 2013-451

Article 74 : « L'autorité compétente, sur réquisition du procureur ou ordonnance du juge d'instruction, peut requérir :

- **de toute personne physique ou morale, l'obligation de communiquer des données spécifiées, en sa possession ou sous son contrôle, qui sont stockées dans un système d'information ou un support de stockage informatique;**
- **d'un fournisseur de services, de communiquer les données spécifiées relatives au trafic et aux abonnés en sa possession ou sous son contrôle ».**

Article 1 , données relatives aux abonnés :
« toute information, sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de services et se rapportant aux abonnés de ses services, autres que des données relatives au trafic ou au contenu, et permettant d'établir sur la base d'un contrat ou d'un arrangement de services :

- le type de service de communication, les dispositions techniques prises à cet égard et la période de service ;
- l'identité, l'adresse postale ou géographique, le numéro de téléphone et tout autre numéro d'accès, les informations relatives à la localisation, la facturation et à l'endroit où se trouvent les équipements de communication ».

50

50

Examen de la législation nationale: Droit procédural

Article 19 – Perquisition et saisie de données informatiques stockées

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à perquisitionner ou à accéder d'une façon similaire:

a à un système informatique ou à une partie de celui-ci ainsi qu'aux données informatiques qui y sont stockées; et

b à un support du stockage informatique permettant de stocker des données informatiques

sur son territoire.

Examen de la législation nationale: Droit procédural

Article 19 – Perquisition et saisie de données informatiques stockées

….

2 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour veiller à ce que, lorsque ses autorités perquisitionnent ou accèdent d'une façon similaire à un système informatique spécifique ou à une partie de celui-ci, conformément au paragraphe 1.a, et ont des raisons de penser que 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,** lesdites autorités soient en mesure d'étendre rapidement la perquisition ou l'accès d'une façon similaire à l'autre système

Examen de la législation nationale: Droit procédural

Loi 2013-451

Article 75 : « L'autorité compétente peut, au cours d'une perquisition effectuée dans les conditions prévues par le code de procédure pénale, accéder à un système d'information ou à un support de stockage numérique et à des données intéressant l'enquête en cours et stockées dans ledit système ou ledit support se trouvant sur les lieux de la perquisition.

L'autorité compétente peut également accéder à des données intéressant **l'enquête en cours et stockées dans un autre système d'information, dès lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial**.

S'il est avéré que ces données, accessibles à partir du système initial ou disponibles pour le système initial, sont stockées dans un autre système d'information situé **hors du territoire national**, elles sont recueillies par l'autorité compétente, **sous réserve du respect des engagements internationaux** ».

53

53

Examen de la législation nationale: Droit procédural

Convention de Budapest Article 15 – Conditions et sauvegardes

1 Chaque Partie veille à ce que l'instauration, la mise en œuvre et l'application des pouvoirs et procédures prévus dans la présente section soient soumises aux conditions et sauvegardes prévues par son droit interne, 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 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.

2 Lorsque cela est approprié, eu égard à la nature de la procédure ou du pouvoir concerné, ces conditions et sauvegardes incluent, entre autres, 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 en question.

3 Dans la mesure où cela est conforme à l'intérêt public, en particulier à la bonne administration de la justice, chaque Partie examine l'effet des pouvoirs et procédures dans cette section sur les droits, responsabilités et intérêts légitimes des tiers.

54

54

Examen de la législation nationale: Droit procédural

Loi 2013-451

Les opérations susceptibles d'être conduites en application du chapitre VIII de la loi font l'objet d'un encadrement font l'objet d'un encadrement juridique. En effet, toutes les mesures ordonnées doivent être conformes au Code de procédure pénale. Ainsi, par exemple, la mise en oeuvre de certaines procédures est subordonnée à l'intervention de l'autorité judiciaire.

Voir par exemple :

Article 74 : « L'autorité compétente, **sur réquisition du procureur ou ordonnance du juge d'instruction**, peut requérir :

- de toute personne physique ou morale, l'obligation de communiquer des données spécifiées, en sa possession ou sous son contrôle, qui sont stockées dans un système d'information ou un support de stockage informatique;

55

Examen de la législation nationale: Droit procédural

Convention de Budapest	Législation nationale
Article 16 – Conservation rapide de données informatiques stockées	Loi 2013-451 Articles 73 et 78 ✓
Article 17 – Conservation et divulgation rapides de données relatives au trafic	Articles 73, 74 et 78
Article 18 – Injonction de produire	Articles 74 ✓
Article 19 – Perquisition et saisie de données informatiques stockées	Articles 71, 74 et 75 ✓
Article 20 – Collecte en temps réel des données relatives au trafic	Article 77 ✓
Article 21 – Interception de données relatives au contenu	Article 77 ✓
Article 22 – Compétence	Article 3 et 41 ✓

56

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	

57

Coopération Internationale

La loi relative à la lutte contre la cybercriminalité ne prévoit pas de dispositions spécifiques relativement à l'entraide.

Cette entraide se fera, comme s'agissant de l'extradition, en vertu d'accord de coopération judiciaire.

58

Examen de la législation nationale: conclusion

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

59

12 mars 2019, Abidjan, Côte d'Ivoire
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 de la Côte d'Ivoire
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 la Côte d'Ivoire**

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE
1949 2019

www.coe.int/cybercrime

60

Conclusions

Discussion:

Quelle voie à suivre pour la Côte d'Ivoire?

61

62