1-2 avril 2019, Conakry, République de Guinée
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 République de Guinée
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 République de Guinée

www.coe.int/cybercrime

1

1-2 avril 2019, Conakry, République de Guinée
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 République de Guinée
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 République de Guinée

www.coe.int/cybercrime

2

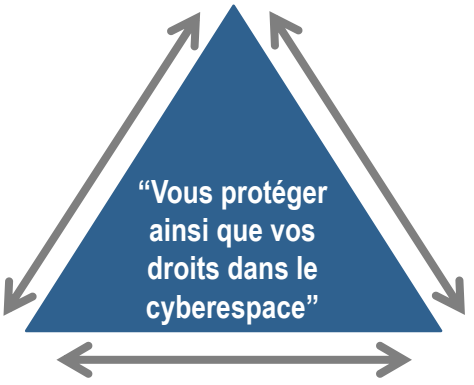
Coopération contre la cybercriminalité: l'approche du Conseil de l'Europe

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 Coopération 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 invités à adhérer
- Portée
  - Droit pénal matériel
  - Droit procédural (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 législation nationale
2. Une fois la législation nationale adoptée, et les capacités de coopérer disponibles, 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 effectue les consultations et pose la question au Comité des Ministres
4. Après un vote positif le pays est invité à accéder (valide pour 5 ans)
5. Le pays est alors libre de décider quand accéder, c'est-à-dire quand 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

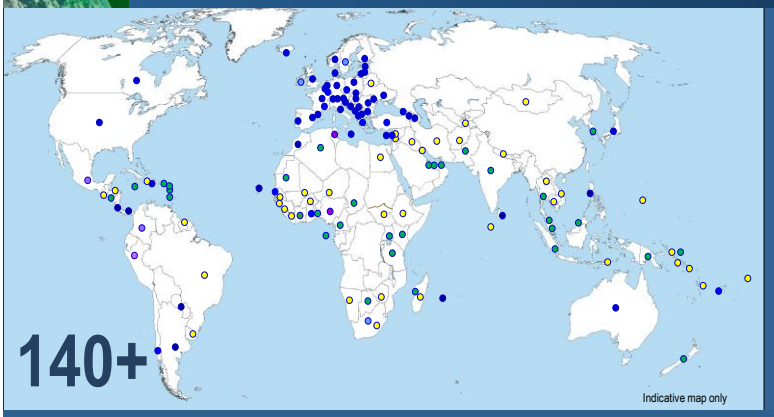
+

Preuves électroniques

- 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 faisant usage de la Convention de Budapest



Etats parties:

- ✓ Cap Vert
- ✓ Ghana
- ✓ Maurice
- ✓ Maroc
- ✓ Sénégal

Signé / invités a adhérer:

- ○ Nigéria
- ○ Afrique du sud
- ○ Tunisie

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

- ► 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

10

Coopération contre la cybercriminalié: renforcer les capacités

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

2 Suivi: Cybercrime Convention Committee (T-CY)

3 Coopération technique/ Capacity building ▶ C-PROC

11

C-PROC: fonctions

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

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: fonctions

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 en cybercriminalité et améliorer la coopération inter-institutionnelle**
- **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 répond aux exigences de l'état de droit
- ✓ Coopération fiable et efficace entre les Etats 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

1-2 avril 2019, Conakry, République de Guinée
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 République de Guinée**
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 République de Guinée

www.coe.int/cybercrime

16

Discussion:

- Quels sont les principaux défis pour la République de Guinée 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 criminels
- 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
- Démocratie
- 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 (preuves électroniques):

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 se trouvent les preuves électroniques?

- 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 dans différentes juridictions
  - Question de savoir quel fournisseur, pour quels services contrôle quelles données
  - Les données sont-elles stockées ou en transit ▶ ordres de production, perquisition / saisie ou interception?

20

Cybercriminalité et preuve électronique: Les défis de la justice pénale

Problèmes spécifiques à résoudre:

- Distinction informations relatives aux abonnés / données de trafic / données de contenu
- Efficacité limitée de l'entraide judiciaire internationale
- 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

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%

22

► Solutions proposées dans le cadre de la Convention de Budapest

1. Solutions:
   Une coopération internationale 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: Protocole

A. Dispositions pour une coopération internationale plus efficace

- Coopération internationale accélérée pour les informations relatives aux abonnés
- Injonctions de 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 présents dans 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

Défis

Janvier 2013	Etats	Législation largement conforme		Législation partiellement conforme		Aucune legislation ou pas d'information	
Afrique	54	6	11%	18	33%	30	56%
Amérique	35	10	29%	12	34%	13	37%
Asie	42	13	31%	17	40%	12	29%
Europe	48	38	79%	8	17%	2	4%
Océanie	14	3	21%	6	43%	5	36%
Total	**193**	**70**	**36%**	**61**	**32%**	**62**	**32%**

Janvier 2018	Etats	Législation largement conforme		Législation partiellement conforme		Aucune legislation ou pas d'information	
Afrique	54	14	26%	21	39%	19	35%
Amérique	35	14	40%	15	43%	6	17%
Asie	42	17	40%	18	43%	7	17%
Europe	48	44	92%	4	8%	0	0%
Océanie	14	5	36%	6	43%	3	21%
Total	**193**	**94**	**49%**	**64**	**33%**	**35**	**18%**

www.coe.int/cybercrime

25

Défis

► Préoccupation: lois sur la cybercriminalité utilisées pour censurer le discours public

- La protection de la sécurité nationale et de l'ordre public est un motif de restriction valable de la liberté d'expression dès lors que cette est restriction est:
  - Prévue par la loi
  - Nécessaire dans une société démocratique
  - Proportionnelle
- Des dispositions trop larges, vagues et imprécises ne remplissent pas ces trois conditions cumulatives
  - "use of computers with intent to compromise the independence of the state or its unity, integrity, safety or any of its high economic, political, social, military or security interests or subscribe, participate, negotiate, promote, contract or deal with an enemy in any way in order to destabilise security and public order or expose the country to danger …"
  - "use of computers to create chaos in order to weaken the trust of the electronic system of the state or provoke or promote armed disobedience, provoke religious or sectarian strife, disturb public order, or harm the reputation of the country … "
  - "creation of sites with a view to disseminating ideas contrary to public order or morality"
- Tendance actuelle problématique ► discrédite l'action légitime de la lute contre la cybercriminalité ► violation des libertés fondamentales

26

Défis

Pouvoirs procéduraux spécifiques	Etat	Janvier 2013 Largement conforme		Janvier 2018 Largement conforme	
Afrique	54	5	*9%*	10	*19%*
Amérique	35	5	*14%*	9	*26%*
Asie	42	8	*19%*	13	*31%*
Europe	48	31	*65%*	39	*81%*
Océanie	14	1	*7%*	3	*21%*
Total	**193**	**50**	***26%***	**74**	***38%***

- Exemples de bonnes pratiques en Afrique
- De plus en plus de législations relatives à la protection des données
- Convention sur la protection des données 108: Cap Vert, Maurice, Maroc, Sénégal + soutien apporté au Kenya et Nigéria

- Trop souvent recours aux pouvoirs généraux
- Problème de sauvegardes

27

Cybercriminalité et preuves électroniques: Réponses de Guinée

Discussion: Quelles sont les réponses de la République de Guinée?

Législation:

- Loi n° L/2016/037/AN du 28 juillet 2016 relative à la cyber-sécurité et la protection des données à caractère personnel
- Code pénal
- Code de procédure pénale
- Loi n° L/2017/023/AN du 16 juin 2017 autorisation la ratification de la Convention de l'Union africaine sur la cyber-sécurité et la protection des données à caractère personnel
- Autres?

Institutions, rôles, responsabilités?

- Agence Nationale de Sécurité des Systèmes d'Information (ANSSI)
- (future) Brigade Nationale de lutte contre la Cybercriminalité
- Plateforme de lutte contre la cybercriminalité (CERT) [article 92 Loi L/2016/037/AN]

Défis?

www.coe.int/cybercrime

28

1-2 avril 2019, Conakry, République de Guinée
Organisé dans le cadre du projet Cybercrime@Octopus

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 République de Guinée
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 République de Guinée

www.coe.int/cybercrime

29

Examen de la législation nationale: Droit pénal matériel

Convention de Budapest	Législation nationale
Article 2 – Accès illégal	L/2016/037/AN/P1 : articles 4 et 5 Code pénal: articles 857 et 868
Article 3 – Interception illégale	L/2016/037/AN/P1 : article 11 Code pénal: article 868
Article 4 – Atteinte à l'intégrité des données	L/2016/037/AN/P1 : article 12
Article 5 – Atteinte à l'intégrité du système	L/2016/037/AN/P1 : articles 8 et 9 Code pénal: articles 858, 859 et 870
Article 6 – Abus de dispositifs	L/2016/037/AN/P1 : articles 17, 18 et 19 Code pénal: articles 860 et 878
Article 7 – Falsification informatique	L/2016/037/AN/P1 : article 13
Article 8 – Fraude informatique	L/2016/037/AN/P1 : article 16
Article 9 – Infractions se rapportant à la pornographie enfantine	L/2016/037/AN/P1 : articles 1, 22, 23 et 24 Code de l'enfant: article 360 Code pénal: article 873
Article 10 – Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes	L/2016/037/AN/P1 : articles 58 et 59

30

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. »

31

Examen de la législation nationale: Droit pénal matériel

Code pénal

Article 857: « Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données, est puni d'un emprisonnement de 2 ans et d'une amende de 10.000.000 de francs guinéens ou de l'une de ces deux peines seulement. »

Article 858: « Est puni des peines prévues á l'alinéa 1 ci-dessus [emprisonnement de 5 à 10 ans et/ou amende de 50.000.000 à 100.000.000 de francs guinéens] tout accès non autorisé à l'ensemble ou à une partie du réseau de communication électroniques ou d'un système d'information ou d'un équipement terminal.
Les peines prévues à l'alinéa 1, sont doublées en cas d'accès illicite portant atteinte à l'intégrité, la confidentialité, la disponibilité du réseau de communications électroniques ou du système d'information
Est puni des peines prévues à l'alinéa 1, quiconque s'introduit sans droit dans un réseau de communications électroniques ou dans un système d'information par défi intellectuel. »

32

Examen de la législation nationale: Droit pénal matériel

Loi L/ 2016/037/AN/P1

Article 4 : Quiconque accède ou tente d'accéder frauduleusement à tout ou partie d'un système informatique, pour quelles que raisons que soient, commet une infraction condamnée et punie par la loi.

Article 5:, Est puni d'un emprisonnement de un (1) an à cinq (5) ans et d'une amende de 60.000.000 à 130.000.000 Francs guinéens quiconque tente d'accéder frauduleusement à tout ou partie d'un système informatique.

Toute personne complice de la commission de cette infraction, sera punie des mêmes peines.

Article 6: Quiconque se maintient ou tente de se maintenir frauduleusement dans tout ou partie d'un système informatique, sera puni d'un emprisonnement de deux (2) ans à cinq (5) ans et d'une amende de 80.000.000 à 150.000.000 Francs guinéens.

Toute personne complice de la commission de cette infraction, sera punie des mêmes peines.

33

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. »

34

Examen de la législation nationale: Droit pénal matériel

Loi L/ 2016/037/AN/P1

Article 11: « 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 informatique, sera puni d'un emprisonnement de 5 à 10 ans et d'une amende de 500.000.000 à 1.000.000.000 Francs Guinéens. Toute personne complice de la commission de cette infraction, sera punie des mêmes peines. »

35

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. »

36

Examen de la législation nationale: Droit pénal matériel

Loi L/2016/037/AN/P1

Article 12:« Quiconque altère ou tente d'altérer, modifie ou tente de modifier, supprime ou tente de supprimer frauduleusement des données informatisées, sera puni d'un emprisonnement de 5 à 10 ans et d'une amende de 500.000.000 à 1.000.000.000 francs guinéens.
Toute personne complice de la commission de cette infraction, sera punie des mêmes peines. »

37

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. »

38

Examen de la législation nationale: Droit pénal matériel

Loi L/2016/037/AN/P1

Article 8: « Quiconque entrave, fausse ou tente d'entraver ou de fausser le fonctionnement d'un système informatique, sera puni d'un emprisonnement de 3 à 6 ans et d'une amende de 100.000.000 à 500.000.000 francs guinéens.
Toute personne complice de la commission de cette infraction, sera punie des mêmes peines. »

Article 9: « Quiconque introduit ou tente d'introduire frauduleusement des données dans un système informatique, sera puni d'un emprisonnement de 3 à 6 ans et d'une amende de 100.000.000 à 500.000.000 francs guinéens.
Toute personne complice pour la commission de cette infraction, sera punie des mêmes peines »

39

Examen de la législation nationale: Droit pénal matériel

Code pénal

Article 858: « Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni d'un emprisonnement de 5 ans et de 40.000.000 de francs guinéens ou de l'une de ces deux peines seulement.
Lorsque cette infraction est commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à 7 ans d'emprisonnement et l'amende à 50.000.000 de francs guinéens ou de l'une de ces deux peines seulement. »

Article 859: « 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 d'un emprisonnement de 5 ans et d'une amende de 40.000.000 de francs guinéens ou de l'une de ces deux peines seulement.
Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à 5 ans d'emprisonnement et l'amende à 50.000.000de francs guinéens ou de l'une de ces deux peines seulement. »

40

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. »

41

Examen de la législation nationale: Droit pénal matériel

Code pénal

Article 860: « Le fait, sans motif légitime, notamment de recherche ou de sécurité informatique, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les dispositions du présent code, est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée. »

Article 878: « Est puni des peines prévues à l'article 872 [1 à 2 ans d'emprisonnement et/ou amende de 10.000.000 à 50.000.000 francs guinéens], quiconque importe, détient, offre, cède, vend ou met à disposition, sous quelque forme que ce soit, un programme informatique, un mot de passe, un code d'accès ou toutes données informatiques similaires conçus et ou spécialement adaptés, pour permettre d'accéder, à tout ou partie d'un réseau de communications électroniques ou d'un système d'information dans l'intention de porter atteinte à l'intégrité des données. »

42

Examen de la législation nationale: Droit pénal matériel

Budapest Article 7 – Falsification informatique

« Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'introduction, l'altération, l'effacement ou la suppression intentionnels et sans droit de données informatiques, engendrant des données non authentiques, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient authentiques, qu'elles soient ou non directement lisibles et intelligibles. Une Partie peut exiger une intention frauduleuse ou une intention délictueuse similaire pour que la responsabilité pénale soit engagée. »

43

Examen de la législation nationale: Droit pénal matériel

Loi L/2016/037/AN/P1

Article 13: « Quiconque produit ou fabrique un ensemble de données par l'introduction, la modification, l'altération ou la suppression frauduleuse de données informatiques, engendrant des données contrefaites, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient originales, sera puni d'un emprisonnement de 5 à 10 ans et d'une amende de 500.000.000 à 1.000.000.000 francs guinéens.

Toute personne complice de la commission de cette infraction, sera punie des mêmes peines. »

44

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. »

45

Examen de la législation nationale: Droit pénal matériel

Loi L/2016/037/AN/P1

Article 16: « Quiconque obtient frauduleusement, pour soi-même 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 fonctionnement d'un système informatique, sera puni d'un emprisonnement de 2 à 5 ans et d'une amende de 400.000.000 à 700.000.000 francs guinéens.

Toute personne complice de la commission de cette infraction sera punie des mêmes peines. »

46

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.

47

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. »

48

Examen de la législation nationale: Droit pénal matériel

Loi L/2016/037/AN/P1

Article 1: « Au sens de la présente loi, les termes ci-dessous sont entendus de la manière suivante : […]
Mineur : toute personne âgée de moins de 18 ans au sens du Code pénal guinéen
Pornographie infantile : toute donnée quelle qu'en soit la nature ou la forme, représentant de manière visuelle un mineur se livrant à un agissement sexuellement explicite ou des images représentant un mineur se livrant à un comportement sexuellement explicite. »

Article 22: « Quiconque produit, enregistre, met à disposition, diffuse, transmet une image ou une représentation présentant un caractère de pornograpie infantile par le biais d'un système informatique ou d'un moyen de stockage de données informatiques, se rend coupable de délit et sera puni d'un emprisonnement de 5 à 10 ans et d'une amende de 700.000.000 à 1.000.000.000 francs guinéens.
Toute personne complice de la commission de cette infraction sera punie des mêmes peines, mais également de toute personne qui tenterait commettre cette infraction. »

49

Examen de la législation nationale: Droit pénal matériel

Loi L/2016/037/AN/P1

Article 23: « 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 informatique ou d'un moyen de stockage de données informatiques, sera puni d'un emprisonnement de 5 à 10 ans et d'une amende de 700.000.000 à 1.000.000.000 francs guinéens.
Toute personne complice pour la commission de cette infraction, sera punie des mêmes peines, au même titre que toute personne qui tenterait de commettre cette infraction. »

Article 24: « Quiconque possède intentionnellement une image ou une représentation présentant un caractère de pornographie infantile par le biais d'un système informatique ou d'un moyen de stockage de données informatiques, sera puni d'un emprisonnement de 2 à 5 ans et d'une amende de 250.000.000 à 500.000.000 francs guinéens ou de l'une de ces deux peines seulement.
Toute personne complice de commission de cette infraction sera punie des mêmes peines. »

50

Examen de la législation nationale: Droit pénal matériel

Code de l'enfant

Article 360: « Sont considérés comme infractions et réprimés conformément aux peines portées à l'article 359 ci-dessus [emprisonnement de 1 à 5 ans et amende de 300.000 à 1.000.000 de francs guinéens], les comportements suivants :
1. La production de pornographie enfantine en vue de sa diffusion par la biais d'un système informatique ;
2. L'offre ou la mise à disposition de pornographie enfantine par le biais d'un système informatique ;
3. La diffusion ou la transmission de pornographie enfantine par le biais d'un système informatique ;
4. Le fait de se procurer ou de procurer à autrui de la pornographie enfantine par le biais d'un système informatique ;
5. La possession de pornographie enfantine dans un système informatique ou un moyen de stockage de données informatiques ;
6. La représentation de manière visuelle : d'un enfant se livrant à un comportement sexuel explicite, d'une personne qui apparait comme un enfant se livrant à un comportement sexuellement explicite, des images réalistes représentant un enfant se livrant à un comportement sexuellement explicite. »

51

Examen de la législation nationale: Droit pénal matériel

Code pénal

Article 873: « Les faits de pornographie impliquant des enfants, visés aux articles 359 et suivants du Code de l'enfant sont punis d'un emprisonnement de 5 à 10 ans et d'une amende de 50.000.000 à 100.000.000 francs guinéens ou de l'une de ces deux peines seulement, lorsqu'ils sont commis par voie de communications électroniques ou d'un système d'information. »

52

Examen de la législation nationale: Droit pénal matériel

Convention de Budapest	Législation nationale
Article 2 – Accès illégal	L/2016/037/AN/P1 : articles 4 et 5 ✓ Code pénal: articles 857 et 868 ✓
Article 3 – Interception illégale	L/2016/037/AN/P1 : article 11 Code pénal: article 868✓
Article 4 – Atteinte à l'intégrité des données	L/2016/037/AN/P1 : article 12
Article 5 – Atteinte à l'intégrité du système	L/2016/037/AN/P1 : articles 8 et 9 Code pénal: articles 858, 859 et 870
Article 6 – Abus de dispositifs	L/2016/037/AN/P1 : articles 17, 18 et 19 ✓ Code pénal: articles 860 et 878 ✓
Article 7 – Falsification informatique	L/2016/037/AN/P1 : article 13
Article 8 – Fraude informatique	L/2016/037/AN/P1 : article 16
Article 9 – Infractions se rapportant à la pornographie enfantine	L/2016/037/AN/P1 : articles 1, 22, 23 et 24 Code de l'enfant: article 360 Code pénal: article 873
Article 10 – Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes	L/2016/037/AN/P1 : articles 58 et 59 ✓

53

Examen de la législation nationale: Droit pénal matériel

Convention de Budapest	Législation nationale
Article 11 – Tentative et complicité	Tentative: ✓ Complicité: ✓
Article 12 – Responsabilité des personnes morales	L/2016/037/ANP1 Article 3 ✓ Code pénal Article 16 ✓

54

Examen de la législation nationale: Droit pénal matériel

Dispositions nationales additionnelles

Article 31: La production, la diffusion, la mise à disposition d'autrui des données de nature à troubler l'ordre ou la sécurité publics ou à porter atteinte à la dignité humaine par le biais d'un système informatique, se rend coupable de délit, et sera puni par la loi.

Article 32: Quiconque produit, diffuse ou met à disposition d'autrui des données de nature à troubler l'ordre ou la sécurité publics ou à porter atteinte à la dignité humaine par le biais d'un système informatique, se rend coupable de délit, et sera puni d'un emprisonnement de six (6) mois à cinq (5) ans et d'une amende de 20.000.000 à 300.000.000 Francs Guinéens.

Cette peine pourra être aggravée en fonction de l'ampleur de l'infraction et du préjudice causé. Toute personne complice pour la commission de cette infraction, sera punie des mêmes peines.

55

Examen de la législation nationale: Droit pénal matériel

Article 41: Quiconque commet ou tente de commettre un acte de terrorisme visant des données, logiciels et/ou programmes informatiques pourrait être assimilé à un crime, entraînant selon l'ampleur de l'infraction, un emprisonnement de cinq (05) ans à dix (10) ans et une amende de 500.000.000 à 3.000.000.000 Francs Guinéens.

Toute personne complice de la commission de cette infraction sera punie des mêmes peines.

56

Examen de la législation nationale: Droit pénal matériel

- Dispositions trop larges qui laissent place à une trop grande interprétation
- L'imprécision et le caractère trop vague de certaines dispositions engendrent une insécurité juridique
- Le manque de prévisibilité juridique est préjudiciable aux justiciables

→ Contraire aux principes de l'état de droit

57

Examen de la législation nationale: Droit procédural

Convention de Budapest	Législation nationale
Article 16 – Conservation rapide de données informatiques stockées	L/2016/037/AN/P1 : articles 97 et 100
Article 17 – Conservation et divulgation rapides de données relatives au trafic	
Article 18 – Injonction de produire	L/2016/037/AN/P1 : article 101
Article 19 – Perquisition et saisie de données informatiques stockées	L/2016/037/AN/P1 : articles 94 et 102 Code de procédure pénale: article 68, 74, 165 et 169
Article 20 – Collecte en temps réel des données relatives au trafic	L/2016/037/AN/P1 : article 103
Article 21 – Interception de données relatives au contenu	L/2016/037/AN/P1 : article 103
Article 22 – Compétence	L/2016/037/AN/P1 : article 3 Code pénal: article 9-13

58

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.

2. Lorsqu'une Partie fait application du paragraphe 1 ci-dessus, au moyen d'une injonction ordonnant à une personne de conserver des données stockées spécifiées se trouvant en sa possession ou sous son contrôle, cette Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger cette personne à conserver et à protéger l'intégrité desdites données pendant une durée aussi longue que nécessaire, au maximum de quatre-vingt-dix jours, afin de permettre aux autorités compétentes d'obtenir leur divulgation. Une Partie peut prévoir qu'une telle injonction soit renouvelée par la suite.

… »

59

Examen de la législation nationale: Droit procédural

Loi L/2016/037/AN/P1

Article 97: « Lorsque les nécessités de l'information l'exigent et lorsqu'il y a des raisons sérieuses de craindre la disparition des données informatiques archivées valant preuve ou commencement de preuve, l'autorité compétente, peut faire injonction à toute personne intéressée, de conserver et de protéger dans le secret l'intégrité des données en sa possession ou sous son contrôle, dans un délai maximum de 10 ans à compter de la date de la notification de l'injonction. »

Article 100: « Lorsque dans le cadre d'une enquête ou d'une instruction, il existe 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 informatique, sont susceptibles de perte ou de modification, l'autorité compétente peut procéder ou faire procéder à la conservation immédiate desdites données. Une telle décision peut être également ordonnée par l'autorité judiciaire compétente.
La personne physique ou morale à qui injonction est faite, doit conserver et protéger l'intégrité desdites données pendant une durée aussi longue que le temps nécessaire pour l'instruction ou pour l'enquête. »

60

Examen de la législation nationale: Droit procédural

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.

…

61

Examen de la législation nationale: Droit procédural

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. »

62

Examen de la législation nationale: Droit procédural

Loi L/2016/037/AN/P1

Article 1: « « Au sens de la présente loi, les termes ci-dessous sont entendus de la manière suivante : […]
Données relatives aux abonnés : toute information sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de services notamment de communications électroniques/tics, 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 services de communication, les dispositions techniques prises à cet effet, et la durée du service ;
- L'identité, l'adresse postale ou géographique, le numéro de téléphone ou tout autre numéro d'accès, l'adresse email, les informations relatives à la localisation, la facturation et à l'endroit où se trouvent les équipements de la communication. »

63

Examen de la législation nationale: Droit procédural

Loi L/2016/037/AN/P1

Article 101: « L'autorité publique compétente 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 informatique ou un support de stockage informatique ;
- d'un opérateur de systèmes informatiques ou d'un prestataire de services de communications électroniques, de communiquer les données spécifiées relatives au trafic et aux abonnés en sa possession ou sous son contrôle. »

[Question: quelle est « L'autorité publique compétente »?]

64

Examen de la législation nationale: Droit procédural

Convention de Budapest	Législation nationale
Article 16 – Conservation rapide de données informatiques stockées	L/2016/037/AN/P1 : articles 97 et 100
Article 17 – Conservation et divulgation rapides de données relatives au trafic	
Article 18 – Injonction de produire	L/2016/037/AN/P1 : article 101
Article 19 – Perquisition et saisie de données informatiques stockées	L/2016/037/AN/P1 : articles 94 et 102 Code de procédure pénale: article 68, 74, 165 et 169
Article 20 – Collecte en temps réel des données relatives au trafic	L/2016/037/AN/P1 : article 103
Article 21 – Interception de données relatives au contenu	L/2016/037/AN/P1 : article 103
Article 22 – Compétence	L/2016/037/AN/P1 : article 3 ✓ Code pénal: article 9-13 ✓

65

Examen de la législation nationale: Droit procédural

CHAPITRE XIX : ORGANE(S) OU INSTITUTION(S) RESPONSABLES DE LA LUTTE CONTRE LA CYBERCRIMINALITE ET DE LA BONNE APPLICATION DE LA PRESENTE LOI

Article 89: Le Centre de sécurité des systèmes d'information (CERT) est chargé de la prévention (veille), de l'alerte, des investigations, de la recherche, de la détection, de la riposte, du déferrement des suspects, auteurs et leurs complices, de la certification, de la sensibilisation et de la formation en matière de lutte et de répression contre les menaces et infractions aux technologies de l'information et de la communications notamment les systèmes informatiques et les communications électroniques en République de Guinée.

Cette structure est l'organe principalement responsable de la lutte et de la répression contre la cybercriminalité en République de Guinée et dispose à cet égard de tous les pouvoirs requis à cet effet.

Des dispositions règlementaires fixeront les modes de fonctionnement du CERT.

66

Examen de la législation nationale: Droit procédural

CHAPITRE XX :AUTRES MECANISMES ET ACTEURS IMPORTANTS DANS LA LUTTE CONTRE LA CYBERCRIMINALITE

Article 92: Le Ministre des Postes, des Télécommunications et de l'Economie Numérique, en collaboration avec les autres départements concernés devra prendre toutes mesures, décisions utiles et nécessaires, visant à favoriser l'installation et l'opérationnalisation dans de brefs délais à compter de la promulgation de la présente loi, d'une Plateforme de lutte contre la cybercriminalité (CERT) au sein de chaque secteur socio-économique de la Guinée (Opérateurs de Téléphonie, Fournisseurs d'Accès Internet, Banques, Assurances, Universités publiques ou privées, Hôpitaux, Industries d'extraction ou autres Industries de production et de services etc.), afin de leur permettre de renforcer les synergies et mutualiser leurs efforts pour une meilleure lutte contre la cybercriminalité au sein de leurs secteurs d'activités respectifs.

Article 93: Ces plateformes sectorielles de lutte contre la cybercriminalité, vectrices d'efficacité dans la lutte contre la cybercriminalité à l'échelle du territoire national, seront placées sous la coordination du Centre National de sécurité des systèmes d'information.

67

Examen de la législation nationale: Droit procédural

TITRE IV
REGLES PROCEDURALES EN MATIERE DE CYBERCRIMINALITE ET MOYENS DE PREUVES

Article 94: Les Agents assermentés du centre pour la sécurité des systèmes d'information ou les officiers de police judiciaire sur réquisition ou mandat du parquet et sur décision de l'autorité judiciaire compétente selon le cas, peuvent en cas de soupçon fondé ou d'infraction avérée :

- ✓ procéder à des perquisitions ou accéder à tout système informatique, en vue de la manifestation de la vérité ;
- ✓ procéder à la saisie conservatoire ou à la confiscation définitive des équipements, supports, matériels, logiciels, programmes, données, documents, ayant servi à la commission de l'infraction ou qui étaient destinés à la commission d'une infraction (tentative);
- ✓ procéder à la mise sous scellés des locaux ayant abrité la commission de l'infraction ou qui étaient destinés à la commission d'une infraction (tentative).

68

Examen de la législation nationale: Droit procédural

Article 96: Les perquisitions, enquêtes ou accès par les agents ou services compétents à tout système d'information, ne peuvent être opérés en violation des règles prescrites par le Code Pénal et de Procédure Pénale en vigueur en République de Guinée, à l'exception des cas ou situations consécutifs d'un risque ou d'un péril imminent et/ou d'une atteinte grave pour la santé, la sécurité et/ou le bon fonctionnement de l'Etat, ou d'un citoyen.

Les Agents assermentés peuvent à cet effet, librement procéder, seuls ou avec le concours d'autres officiers de police judiciaire ou des forces de défense et de sécurité en général, à des contrôles inopinés, investigations, perquisitions, saisies, arrestations, déferrements de suspects et de leurs complices ou plus généralement, exercer tous pouvoirs de police administrative et judiciaire dans le cyber-espace, dont la mise en œuvre pourrait s'avérer utile ou fondamentale pour la défense des intérêts fondamentaux de la nation, ou la sécurité, la tranquillité et la santé des citoyens.

Toutefois, ces agents demeureront pénalement et civilement responsables de tous abus qu'ils commettraient au cours de l'exercice de ces mesures d'exception.

69

Examen de la législation nationale: Droit procédural

Institutions: quid rôles et responsabilités?

- **Agence Nationale de Sécurité des Systèmes d'Information (ANSSI)**
- **(future) Brigade Nationale de lutte contre la Cybercriminalité**
- **Plateforme de lutte contre la cybercriminalité (CERT) [article 92 Loi L/2016/037/AN]**

Sauvegardes?

70

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	

71

Examen de la législation nationale: Conclusion

- **Droit matériel**
  - Combler les différentes lacunes identifiées
  - Harmoniser les dispositions des instruments législatifs applicables en matière de cybercriminalité, notamment la L/2016/037/AN/P1 et le Code pénal
  - Revoir les peines-menaces applicables
  - Revoir les dispositions sur le contenu (par exemple, articles 31 ss) en vue des conditions de l'Etat de droit
- **Droit procédural**
  - Clarifier les Institutions, rôles, responsabilités
- **Coopération internationale**
  - Prévoir un cadre juridique relatif à la coopération internationale en matière de cybercriminalité

72

1-2 avril 2019, Conakry, République de Guinée
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 République de Guinée
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 République de Guinée**

www.coe.int/cybercrime

73

Conclusions

Discussion:

Quelle voie à suivre pour la République de Guinée?

- Réforme de la législation interne (group de travail)
- Soutien du Conseil de l'Europe à ces réformes
- Carification des compétences pour les enquêtes pénales sur la cybercriminalité
- Mise en place d'une unité spécialisée
- Formation avec le soutien du Conseil de l'Europe
- Adhésion à la Convention de Budapest une fois la législation de réforme achevée

74

75