Policing and prosecuting cybercrime through international cooperation: Prospects and Challenges

Maintien de l'ordre et traduction en justice des cybercriminels grâce à la coopération internationale: perspectives et défis

Dr. Janvier NGNOULAYE

African Union Cyber Security Experts Group, Cyber security specialist
jnoulaye@gmail.com , aucseg@africa-union.org

MAINTIEN DE L'ORDRE DANS LE CYBERESPACE ET TRADUCTION EN JUSTICE DES CYBERCRIMINELS GRÂCE À LA COOPÉRATION INTERNATIONALE: PERSPECTIVES ET DÉFIS

PLAN

- LA CONNECTIVITÉ MONDIALE ET LA CYBERCRIMINALITÉ
- UNE PERSPECTIVE GLOBALE
- LA LÉGISLATION, L'INCRIMINATION ET L'APPLICATION DES LOIS
- LES PREUVES ÉLECTRONIQUES ET LA JUSTICE PÉNALE
- LA COOPÉRATION INTERNATIONALE ET LA PRÉVENTION
- LÉGISLATION MONDIALE SUR LA CYBERCRIMINALITÉ
- CONCLUSION

LA CONNECTIVITÉ MONDIALE ET LA CYBERCRIMINALITÉ

- Depuis 2017, on a estimé à près de 70 % de la population mondiale disposant d'un abonnement au haut débit à Internet.
- Depuis 2020, les dispositifs en réseau comme les objets connectés sont 6 fois plus nombreux que les personnes, et cela transforme les conceptions actuelles de l´internet.
- Un nombre limite d´actes contre la confidentialité, l´intégrité et la disponibilité des données et des systèmes informatiques représentent l´essentiel de la cybercriminalité qui implique les preuves électroniques liées à la connectivité du protocole internet (IP).
- Dans ce monde hyper connecté d'aujourd'hui il est désormais difficile de concevoir clairement un « délit informatique ».

UNE PERSPECTIVE GLOBALE

- On estime que plus de 80 % des actes de cybercriminalité proviennent d´activités organisées.
- Il existe des marches noirs de cybercriminalité établis dans des cycles de création des logiciels malveillants, des infections informatiques, des gestions de botnet (réseau de machines), la récupération des données financières ou personnelles, la vente de données financières et leur encaissement.
- Plus d´un million d´adresses IP uniques fonctionnaient au niveau global comme des serveurs de contrôle et de commandes de botnets en 2011.

UNE PERSPECTIVE GLOBALE

- On estime qu´environ 24 % du trafic global d´internet enfreint le droit d´auteur, en téléchargeant avec du matériel partagé en pair à pair (P2P) et cela est particulièrement fréquent dans des pays d´Afrique
- Les taux de victimisation relative à la cybercriminalité sont plus élevés dans les pays dont le niveau de développement est plus bas, et cela démontre qu´il est nécessaire de renforcer les efforts de prévention dans ces pays.

LA LÉGISLATION, L'INCRIMINATION ET L'APPLICATION DES LOIS

- Des progrès significatifs concernant la promulgation d´instruments régionaux et internationaux visant à lutter contre la cybercriminalité sont survenus lors de la dernière décennie. On peut mentionner cinq instruments régionaux et internationaux :
  - (i) le Conseil de l´Union Européenne,
  - (ii) la Communauté des états indépendants ou l´Organisation de coopération de Shanghai,
  - (iii) les organisations intergouvernementales africaines,
  - (iv) la Ligue des Etats Arabes,
  - (v) les Nations Unies
- On s'accorde à dire que si un contenu est illégal dans un pays mais légal de le produire et de le diffuser dans d´autres pays, les états devront se concentrer sur les mesures de justice pénale dans la juridiction nationale à l´encontre des personnes qui accèdent à ce contenu, plutôt que sur un contenu produit hors du pays.

LA LÉGISLATION, L'INCRIMINATION ET L'APPLICATION DES LOIS

- Les autorités d´application de la loi et les fournisseurs de services internet ont une interaction particulièrement complexe.
- Les fournisseurs de services détiennent les informations des abonnés, la facturation, certains journaux de connexion, des informations relatives a la localisation et le contenu des communications, qui peuvent représenter des preuves électroniques essentielles d´un délit.
- Les obligations légales nationales, la rétention des informations du secteur privé et les politiques de divulgation varient beaucoup selon le pays, le type d´industrie et de données.
- Certains pays utilisent souvent des ordonnances du tribunal pour que les fournisseurs de services leurs transmettent des preuves.

LES PREUVES ÉLECTRONIQUES ET LA JUSTICE PÉNALE

- Les preuves sont les faits pertinents au moyen desquels la culpabilité ou l´innocence d´une personne est établie lors d´un procès. Les preuves électroniques comprennent toutes les preuves existant en forme numérique. Elles peuvent être stockées ou transitoires. Elles peuvent exister sous la forme de fichiers informatiques, de transmissions, de journal, de métadonnées ou de données en réseau.
- La criminalistique numérique se rapporte à la récupération des informations qui sont souvent volatiles ou cryptées. Les experts en criminalistique doivent être disponibles pour reconstituer la preuve afin de faciliter la compréhension et la décision du procureur.
- Les difficultés auxquelles font face les enquêteurs et les procureurs signifient que les taux relatifs aux auteurs d´un cyber délit traduits en justice sont bas.

LES PREUVES ÉLECTRONIQUES ET LA JUSTICE PÉNALE

- En raison des technologies de l´informatique en nuage impliquant le stockage des données dans de multiples centres de données dans divers emplacements géographiques, les modalités formelles et informelles de coopération internationale doivent se consolider entre les pays.
- En raison de la nature volatile des preuves électroniques, la coopération internationale en matière pénale dans le domaine de la cybercriminalité requiert des réponses en temps opportun et la capacité de requérir des mesures d´enquêtes spécialisées, comme la conservation des données informatiques
- L´accès direct aux données extraterritoriales des services répressifs étrangers peut avoir lieu lorsque les enquêteurs utilisent la connexion en direct existante du dispositif d´un suspect, ou lorsque les enquêteurs utilisent des identifiants d´accès aux données légalement obtenues

LES PREUVES ÉLECTRONIQUES ET LA JUSTICE PÉNALE

- Globalement, les divergences sur la portée des dispositions relatives a la coopération dans les instruments bilatéraux et multilatéraux, une absence d´obligation en matière de délai de réponse, une absence d´accords relatifs à l´accès direct autorise aux données extraterritoriales, les multiples réseaux informels des services d´application de la loi, et les variations de garanties en matière de coopération, représentent des difficultés non négligeables pour une coopération internationale efficace pour ce qui concerne les preuves électroniques dans des affaires pénales.

LA COOPÉRATION INTERNATIONALE ET PRÉVENTION

- Avec des serveurs de contenu et réseaux de données éparpillés dans le monde, des actes de cybercriminalité impliquent une dimension transnationale, et met en jeu des questions d´enquêtes transnationales, de souveraineté, de juridiction, de preuves extraterritoriales et de la nécessite de la coopération internationale.
- La dimension transnationale des délits de cybercriminalité surgit lorsqu´un effet important du délit se trouve dans un autre territoire, ou si une partie du *« mode opératoire»* du délit a eu lieu dans un autre territoire.
- Le droit international prévoit certaines bases de juridiction sur ces actes, y compris des formes de juridiction fondée sur le territoire et de juridiction fondée sur la nationalité.
- Certaines de ces bases sont également incluses dans les instruments multilatéraux sur la cybercriminalité

LA COOPÉRATION INTERNATIONALE ET PRÉVENTION

- Les utilisateurs d´internet doivent prendre des précautions basiques de sécurité.
- L´importance constante des campagnes de sensibilisation publiques, y compris celles qui abordent les menaces émergentes et celles qui visent des audiences spécifiques
- L'utilisation de techniques de cyber sécurité comme les pare-feu, la conservation des preuves digitales, l´identification du contenu, la détection des intrusions, la surveillance et le contrôle du système
- Les institutions académiques jouent différents rôles dans la prévention de la cybercriminalité, avec la prestation de services d´éducation et de formation aux professionnels, le développement de politiques et de lois, et des travaux sur les normes techniques et le développement de solutions. Les universités disposent et fournissent des experts en cybercriminalité, des équipes d´intervention informatique d´urgence (CERT) et des centres de recherche spécialisés.

Pourquoi une législation sur la cybercriminalité et les preuves électroniques?

Augmentation massive de la cybercriminalité = infractions contre et au moyen d'ordinateurs

La cybercriminalité liée à COVID-19 : une illustration

Tout crime peut impliquer des preuves sur des systèmes informatiques

La criminalité dans le cyberespace : une menace pour les droits de l'homme, la démocratie et l'État de droit

Une réponse efficace de la justice pénale est nécessaire pour garantir l'État de droit dans le cyberespace

La réponse doit être fondée sur le droit et répondre aux exigences de l'État de droit

Établir les infractions dans le droit pénal matériel

Donner aux services répressifs les pouvoirs nécessaires pour sécuriser les preuves sur les systèmes informatiques

Limiter ces pouvoirs par des garanties

Permettre une coopération internationale efficace

PERSPECTIVES ET DEFIS

PERSPECTIVES ET DEFIS

PERSPECTIVES ET DEFIS

PERSPECTIVES ET DEFIS

African Union

Convention de Budapest : Référence mondiale pour la législation sur la cybercriminalité

Droit pénal matériel

- Accès illégal
- Interception illégale
- Atteinte à l'intégrité des données
- Atteinte à l'intégrité du système
- Abus de dispositifs
- Falsification informatique
- Fraude informatique
- Pornographie enfantine
- Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes

+

Droit procédural

- Conservation rapide de données
- Injonction de produire
- Perquisition et saisie de données
- Interception des données relatives au contenu

- Limitée par des garanties

+

Coopération internationale

- Extradition
- MLA
- Informations spontanées
- Conservation rapide
- MLA pour l'accès aux données informatiques
- MLA pour l'interception
- Des points de contact 24 heures sur 24, 7 jours sur 7

Harmonisation

Pouvoirs procéduraux et coopération internationale pour toute infraction pénale impliquant des preuves sur un système informatique !

African Union

Situation mondiale de la législation sur la cybercriminalité

Réformes de la législation sur la cybercriminalité et les preuves électroniques

		Réformes en cours ou entreprises ces dernières années					
	États	En Janvier 2013		En Janvier 2018		En Février 2020	
Afrique	54	25	46%	45	83%	46	85%
Amérique	35	25	71%	31	89%	32	91%
Asie	42	34	81%	37	88%	38	90%
Europe	48	47	98%	48	100%	48	100%
Océanie	14	12	86%	12	86%	13	93%
Tous	193	143	74%	173	90%	177	92%

En février 2020, 177 États membres des Nations unies (soit 92 %) étaient en train d'entreprendre des réformes de la législation sur la cybercriminalité et les preuves électroniques ou avaient entrepris de telles réformes au cours des dernières années.

Situation mondiale de la législation sur la cybercriminalité

Liens vers la Convention de Budapest

		Utilisation de la Convention de Budapest comme ligne directrice ou source					
États		En Janvier 2013		En Janvier 2018		En Février 2020	
Afrique	54	21	39%	33	61%	38	70%
Amérique	35	22	63%	24	69%	26	74%
Asie	42	25	60%	27	64%	28	67%
Europe	48	46	96%	47	98%	47	98%
Océanie	14	10	71%	11	79%	14	100%
Tous	193	124	64%	142	74%	153	79%

- Impact global de la Convention de Budapest en termes de législation ▸ une ligne directrice ou une source d'inspiration pour la législation nationale dans 153 États (soit 79%)

CONCLUSION

Un meilleur maintien de l'ordre dans le cyberespace et la traduction en justice des cybercriminels passerait par:

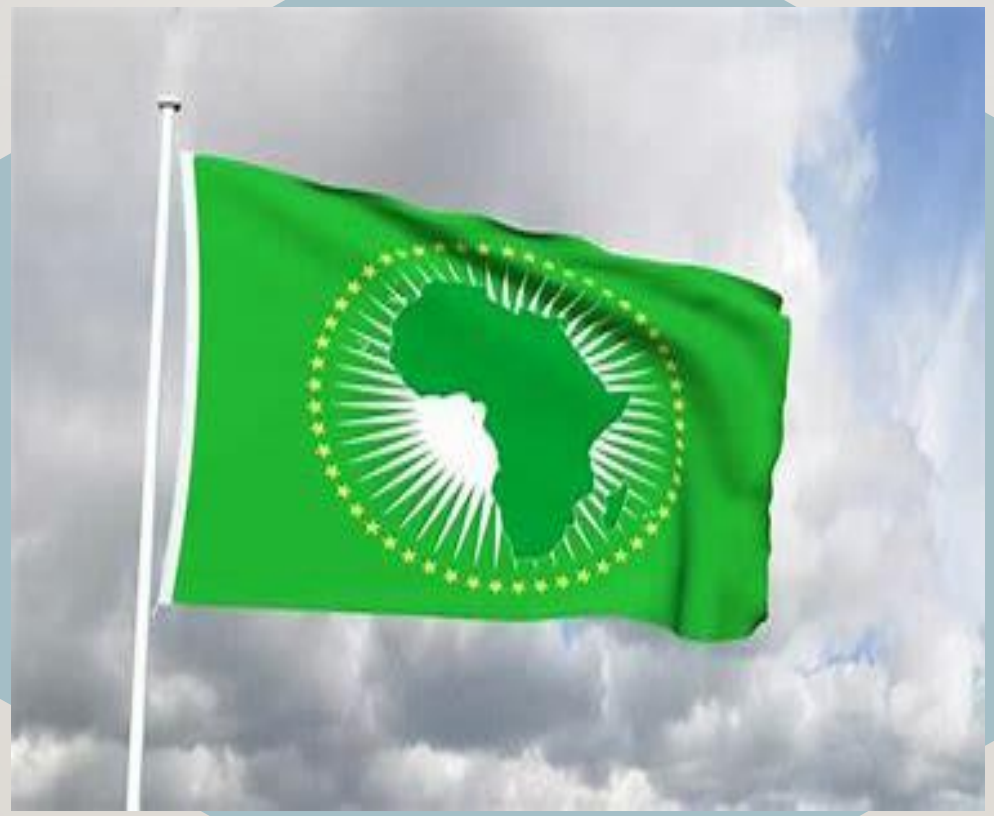
- **La force de la coopération internationale à consolider entre**
  - **pays,**
  - **groupement sous régional,**
  - **groupement régional**
  - **fournisseurs de services pour la gestion des cas d'urgence**

  avec comme ligne directrice la convention de Budapest/Malabo
- **La formation et la sensibilisation des utilisateurs au niveau local (universités, entreprises, administrations publiques et privées, etc.) garantissant la prévention**
- **Le renforcement des capacités pour permettre aux autorités de justice pénale d'appliquer la législation dans la pratique.**
- **Former des experts en criminalistique et les équiper**
- **Partager des meilleurs pratiques lors des rencontres régionales et internationales**

REFERENCES

1. *Étude détaillée sur la cybercriminalité, Ébauche, Février 2013 Office des Nations Unies contre la drogue et le crime - Vienne*
2. *État de la législation mondiale sur la cybercriminalité, Alexander Seger, Conseil de l'Europe*

Thank you, for your attention



Merci pour votre attention

شكرا لك على انتباهك

Obrigado pela sua atenção

aucseg@africa-union.org