**Commissaire Moustapha DIOUF**
**Alumni Master Défense Sécurité et Paix**
**Promotion 2016-2017**
**Centre des Hautes Etudes de Défense et de Sécurité (CHEDS)**

*********

# Cybercriminalité, l'affaire de tous ?

**<u>Question 1</u> : Pour vous, comment pourrait-on définir la Cybercriminalité ?**

Si aujourd'hui les opportunités infinies du numérique ne sont plus à démontrer, dans leurs diverses dimensions politique, socioculturelle, économique et scientifique pour l'humanité qui en fait un bon usage, force est de reconnaitre l'ampleur et la gravité du risque numérique tant pour les organisations que pour les individus. Ainsi, le cyber espace a donné naissance à une nouvelle forme de criminalité appelée cybercriminalité ou encore criminalité informatique qui bouleverse les paradigmes classiques du droit criminel. C'est pourquoi, on en note une variété de définitions suivant les critères établis par chaque Etat, dont on pourra retenir quelques-unes ici :

- Selon le **droit positif sénégalais**, la cybercriminalité est toute infraction qui implique l'utilisation des technologies de l'information et de la communication ;

- **Vincent Lemoine** définit la cybercriminalité comme un ensemble d'atteintes aux biens et aux personnes commises via l'utilisation des nouvelles technologies ;

- Selon le **Ministère de l'Intérieur français**, la cybercriminalité concerne l'ensemble des infractions pénales susceptibles de se commettre sur les réseaux de télécommunication en général, et en particulier sur les réseaux utilisant le protocole TCP-IP appelé communément internet ;

- Pour **Stanislas de Maupeou**, la cybercriminalité peut être définie comme des actes contrevenants aux traités internationaux et aux lois nationales utilisant les réseaux ou les systèmes d'information comme moyen de réalisation d'un délit ou d'un crime, ou ayant ces mêmes réseaux ou systèmes pour cible.

**<u>Question 2 :</u> Quelles sont les typologies de cybercriminalité au Sénégal ?**

On pourrait distinguer trois types ou catégories de cybercriminalité : la cybercriminalité individuelle (contre les personnes), la cybercriminalité contre la propriété et la cybercriminalité gouvernementale :

- **Cybercriminalité individuelle ou contre la personne**

Elle implique une personne qui distribue des informations malveillantes ou illégales en ligne. Il peut s'agir de cyberharcèlement, de distribution de pornographie ou tout simplement de diffusion de données à caractère personnel.

- **Cybercriminalité contre la propriété**

Il peut s'agir d'un cas réel où un criminel possède illégalement les coordonnées bancaires ou de carte de crédit d'une personne. Le pirate vole les coordonnés bancaires d'une personne pour avoir accès à des fonds, faire des achats en ligne ou lancer des arnaques par hameçonnage (phishing) afin d'inciter les gens à divulguer leurs informations. Il pourrait également utiliser un logiciel malveillant pour accéder à une page Web contenant des informations confidentielles.

- **Cybercriminalité gouvernementale**

Cette catégorie est moins répandue, mais elle est la plus grave. Elle comprend le piratage de sites Web gouvernementaux, de sites militaires ou la diffusion de propagande. Ces criminels sont habituellement des terroristes ou des gouvernements ennemis d'autres pays. Ce type de cybercriminalité n'est pas encore répandue au Sénégal.

**<u>Question 3</u> : Quelle stratégie nationale développer pour une lutte efficace contre la cybercriminalité ?**

Dans ce contexte où le Sénégal est engagé comme beaucoup d'autres pays dans la transition numérique avec une administration et une population, de plus en plus connectées, le développement d'une stratégie contribuerait à répondre efficacement aux enjeux de sécurité du numérique. Il pourrait s'agir de réfléchir plus spécifiquement sur les actions pouvant permettre de :

- Gérer les risques liés à la sécurité de notre système d'information (protections des installations informatiques et des données informatisées) ;
- Identifier les principales attaques et menaces sur la sécurité individuelle et celle des services ;
- Développer des techniques d'investigations numériques solides ;
- Renforcer les mécanismes opérationnels d'entraide judiciaire
- Promouvoir la coopération internationale dans un sens favorable à l'émergence d'une approche holistique de la lutte contre la cybercriminalité.

**<u>Question 4</u> : Que peut-on faire pour améliorer la prise de conscience générale des utilisateurs face à la cybercriminalité ?**

Aujourd'hui, diverses infractions sont commises via internet et les réseaux et au moyen de technologies (pédopornographie, intrusion, escroquerie, fraude, injures, diffamation, diffusion de données à caractère personnel etc…).

Cela prouve que la prise de conscience des risques liés à la numérisation de la société reste insuffisante. Face à ce constat, la sensibilisation des masses, le renforcement de capacités des personnels des organisations publiques et privées restent des meilleurs moyens d'asseoir une prise de conscience générale des utilisateurs contre la cybercriminalité.

Moustapha DIOUF
Commissaire de police principal

**<u>Sources</u> :**

Exposé des motifs de la loi n°2008-11 du 25 janvier 2008 portant sur la cybercriminalité,
Voir M. DIOUF, la Police nationale du Sénégal face au défi de la Cybersécurité, abis édition, 2019.