L'expérience du renforcement des capacités

Issa Saferiba FAYAMA, Magistrat, Directeur de Cabinet du Ministre de la Justice, Burkina Faso

I. CONTEXTE DE LA LUTTE CONTRE LA CYBERCRIMINALITE AU BURKINA

A. RAPPORTS AVEC LE CONSEIL DE L'EUROPE

- Avant d'entrer dans les éléments essentiels de mon intervention, je voudrais adresser au conseil de l'Europe à travers les adorables personnes qui l'animent, les profondes gratitudes des plus hautes autorités du Burkina Faso pour l'accompagnement dont le Burkina bénéficie depuis un certain temps de la part du Conseil de l'Europe. Dans le sens de cet accompagnement, la demande d'adhésion du Burkina Faso a été jugée conforme aux instruments juridiques de Budapest et le Burkina a été autorisée à poursuivre le processus d'adhésion et actuellement le Ministère des affaires s'emploie à demander au parlement l'autorisation de ratifier la convention de Budapest et son protocole additionnel.
- Je voudrais terminer ces propos liminaires en ajoutant que courant janvier de cette année une équipe d'experts du conseil de l'Europe a séjourné au Burkina avec pour missions de faire un diagnostic de notre dispositif de lutte contre la cybercriminalité et proposer les correctifs nécessaires. Le COVID a malheureusement ralenti la mise en œuvre de ce processus.

B. PRESENTATION DU DISPOSITIF DE LUTTE CONTRE LA CYBERCRIMINALITE

- Ces précisions étant faites, Il faut dire qu'en matière de **lutte contre la cybercriminalité**, le Burkina Faso ne connait pas comme certains pays Africains, je pense en particulier au Sénégal, une avancée significative alors que le phénomène est réel dans notre pays soit comme victime soit comme pays de départ des actions des cybercriminels. En effet, le dispositif juridique et institutionnel de lutte contre ce phénomène se met en place depuis seulement trois ans.

- En ce qui concerne le **dispositif juridique**, il faut dire que c'est à partir de 2017, avec l'adoption du nouveau code pénal que le Burkina Faso a conformé son droit pénal aux instruments internationaux de lutte contre la cybercriminalité. Et en 2018, toujours avec l'appui du Conseil de l'Europe, la procédure pénale a également été conformée avec les instruments internationaux à savoir la convention de Budapest.

- Sur le **plan institutionnel**, le Burkina a créé seulement en janvier 2020, la brigade centrale de lutte contre la cybercriminalité et qui est en cours d'opérationnalisation.

II. DEFIS BESOINS EN MATIÈRE DE RENFORCEMENT DES CAPACITES

A - AU PROFIT DE LA POLICE JUDICIAIRE

- A travers cette brève présentation du dispositif de lutte contre la cybercriminalité au Burkina Faso qui est vraiment à ses débuts, vous comprenez déjà les défis qui sont les nôtres en termes de renforcement de capacité des ressources humaines notamment.
- En effet, **les besoins de renforcement des capacités** concernent l'ensemble des autorités chargées de l'application de la loi notamment la police judiciaire à former non seulement sur le plan technique mais également sur le plan juridique.
- Sur **le plan technique**, il s'agira de les outiller sur les techniques de traque des cybercriminels et surtout les techniques de constitution, de conservation et de production des preuves électroniques dans le respect des droits humains.

- Le tableau ci-après résume les besoins de la police judiciaire sur le **plan technique** :

Formation d'initiation et de mise à niveau	▪ **La méthodologie de collecte de preuves et d'investigation numérique niveau I ;** ▪ **L'OSINT et l'investigation numérique niveau II ;** ▪ **L'investigation numérique légale niveau avancé ;** ▪ **la téléphonie (smartphones, tablettes, GPS, drone) ;** ▪ **L'investigation numérique à travers Linux (niveau I & II) ;** ▪ **La sténographie, la cryptographie, la blockchain et l'investigation sur les sur les cryptos monnaies ;** ▪ **cyber Dark Web Investigations;** ▪ **database forensic;** ▪ **Advanced Flasher Box and Bootloader for mobile forensics;** ▪ **L'analyse forensic par JTAG, ISP et Chip-OFF.**
Formation de certification	▪ **ISO/CEI 27037:2012, Technologies de l'information – Techniques de sécurité – Lignes directrices pour l'identification, la collecte, l'acquisition et la préservation de preuves numériques ;** ▪ **ISO / IEC 17025 : Gestion des Laboratoires - Lead Auditor** ▪ **CEH: Ethical Hacking.**

Besoins de la police judiciaire (continuation) :

- **Sur le plan du droit pénal et de la procédure pénale**, il s'agira de les doter de connaissances juridiques leur permettant de mener une enquête qui intègre le respect des droits humains, ce qui suppose qu'ils disposent au préalable de prérequis sur les éléments constitutifs des infractions qui se réalisent au moyen des technologies de l'information et de la communication.

II- DEFIS BESOINS EN MATIÈRE DE RENFORCEMENT DES CAPACITES

B. AU PROFIT DES MAGISTRATS

- Quant aux **magistrats** (parquet, juges d'instruction et juges), il s'agira pour eux de recevoir des **formations pointues sur le droit pénal spécial de la cybercriminalité** et la **procédure pénale** y relative. Des connaissances sur les techniques d'enquêtes, de poursuites, d'investigation et d'instruction dans les dossiers relatifs à la cybercriminalité leur permettront d'interagir avec les officiers de police judiciaire dans la conduite des enquêtes qui sont effectuées sous le contrôle des magistrats.

- Il est aussi indispensable d'outiller l'ensemble des acteurs de la lutte sur la **coopération** tant interne c'est-à-dire entre acteurs de la lutte à l'intérieur d'un même pays qu'internationale quand on sait que ce phénomène criminel ne s'exercice pas tout le temps sur le territoire d'un seul Etat.