UNION EUROPEENNE

DELEGATION EN REPUBLIQUE DU BENIN

Formation sur la protection des données et les capacités de police globale au Bénin

Allocution d'ouverture du M Ruben Alba Aguilera, Chef de la Coopération de l'UE au Bénin

Cotonou, le 15 juillet 2020

Excellences en vos grades et qualités respectifs,

Distingués partenaires et participants

Tout protocole observé,

Au nom de l'Union européenne et en particulier de la Délégation de l'UE au Bénin, je vous souhaite la bienvenue à cet atelier que nous lançons aujourd'hui, qui permettra au Bénin et au Burkina Faso, de poser une autre pierre angulaire importante sur la voie du renforcement des législations nationales, afin de lutter efficacement contre la criminalité en ligne tout en protégeant les données des utilisateurs et en garantissant le plein respect des droits de l'homme et les principes de l'état de droit.

Je tiens à exprimer notre gratitude aux autorités des deux pays pour l'hospitalité et le soutien dans l'organisation de cet atelier, mais surtout pour votre ferme engagement dans la construction d'un cyberécosystème mondial plus sûr et apte à garantir que nos économies et nos nations continuent à bénéficier des opportunités offertes par ces technologies. Je souhaite également exprimer notre gratitude au Conseil

de l'Europe, qui est un partenaire de longue date dans divers programmes financés par l'Union européenne dans un certain nombre de domaines clés, tels que la lutte contre la cybercriminalité.

En effet, nous soutenons cet atelier dans le cadre du projet conjoint Action globale de l'UE sur la cybercriminalité, appelé GLACY +. Depuis 2013, GLACY + est le principal programme mondial de soutien aux pays partenaires en Afrique pour renforcer les capacités des États à lutter contre la cybercriminalité. En particulier, le Bénin a été invité à adhérer à la Convention de Budapest en juin 2019, et peut désormais bénéficier du soutien du projet.
Le projet a démarré ainsi ses premières activités nationales, après avoir impliqué le Bénin dans certains événements internationaux, aussi en prévision de l'évaluation nationale qui aura lieu à la fin du mois de juillet 2020 et qui nous permettra d'établir un plan d'action pour le pays.

Nous constatons que le cyberespace a créé une nouvelle dimension pour les acteurs criminels - il a démocratisé non seulement le progrès économique, mais aussi la portée géographique, tout en diminuant considérablement les coûts liés à l'adoption d'un comportement criminel. La cybercriminalité existe depuis environ 45 ans et ne peut donc pas être qualifiée de nouvelle forme de criminalité. Cependant, avec l'évolution de la société de l'information, elle est devenue l'un des plus grands défis pour les systèmes de justice pénale en raison de sa nature trans-juridictionnelle.

La cybercriminalité diminue la confiance dans l'Internet, et elle représente également une menace sérieuse pour les droits

fondamentaux des individus, l'état de droit et les efforts des gouvernements pour fournir des services essentiels à leurs citoyens.

L'infrastructure des TIC et les systèmes numériques ont également incité le crime traditionnel à se propager dans le cyberespace. L'évaluation des menaces réalisée par EUROPOL met en évidence la facilité avec laquelle les criminels adoptent les nouvelles technologies dans leurs modes opératoires ou montent de modèles commerciaux frauduleux avec grande compétence.

Ce que nous constatons maintenant, c'est que les gouvernements du monde entier sont non seulement aux prises avec des niveaux croissants de cybercriminalité, mais ils sont aussi confrontés à l’exigence d'obtenir de preuves électroniques pour tout type de crime. Par exemple - comment sécuriser des preuves électroniques stockées sur des serveurs dans des juridictions étrangères, multiples ou inconnues - c'est-à-dire des données «cloud». Avec de plus en plus d'informations stockées dans des services cloud et la grande mobilité des informations et des criminels, la coopération transfrontalière des forces de l’ordre est aujourd'hui cruciale pour la plupart des enquêtes sur la cybercriminalité.

De toute évidence, l'état de droit est menacé si ce n’est qu’une partie mineure des cybercrimes de faire l'objet d'une enquête et d'un jugement. D'une part, les États risquent de faillir au devoir de protéger les droits des individus et de la société contre la criminalité. D'autre part, la cybercriminalité finit également par générer un coût énorme en opportunités de développement économique.

Le cyberespace fournit une formidable plateforme de développement, étalant des technologies numériques transformatrices, avec de profondes implications mondiales et de nombreux avantages économiques et sociaux. Néanmoins, il y a une prise de conscience croissante que les avantages des TIC ne peuvent se matérialiser dans le vide institutionnel. L'augmentation du nombre d'incidents de cybersécurité qui causent des dommages économiques majeurs à l'économie et à la sécurité mondiales soulignent la nécessité de hiérarchiser les mesures visant à lutter contre ces menaces et de promouvoir des services et des infrastructures numériques sécurisés, ainsi que la nécessité d'une législation pertinente et compatible au niveau international.

La Convention de Budapest sur la cybercriminalité est le principal outil international pour la définition de normes communes de lutte contre la cybercriminalité. Son «traité frère» est la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (plus communément appelée «Convention 108»). Cette convention est le seul instrument multilatéral juridiquement contraignant dans le domaine de la protection de la vie privée et de la protection des données. La Convention 108 a récemment été modernisée en tant que Convention 108+, afin de l'adapter aux nouvelles réalités d'un monde de plus en plus connecté, tout en continuant à soutenir la libre circulation des données et le respect de la dignité humaine.

Actuellement, la Convention 108 compte 55 pays signataires et quelques 25 observateurs - c'est-à-dire déjà une large communauté. La Convention 108+ est également soutenue par l'Union européenne et par

le Rapporteur spécial des Nations Unies sur le droit à la vie privée. En ce sens, la convention 108+ est pleinement compatible avec le cadre juridique de l'UE en matière de protection des données. Nous pouvons donc confortablement affirmer qu'au niveau international, la Convention 108+ contribue à une convergence des normes de protection des données, tout en permettant un environnement ouvert à l'innovation et à une croissance économique inclusive au niveau régional et mondial.

Nous nous engageons donc dans le plaidoyer pour renforcer la législation nationale en matière de protection des données personnelles, ainsi que dans la lutte contre la cybercriminalité. L'arrimage avec les normes internationales en vigueur dans le domaine - à savoir la Convention 108+ et la Convention de Budapest sur la cybercriminalité, qui seront au centre des travaux soutenus par les experts qui nous rejoignent aujourd'hui, et particulièrement important

Je voudrais conclure en soulignant que nous sommes très encouragés par l'approche adoptée pour aborder ces questions de manière globale - en travaillant ensemble au renforcement de la protection des données, de la cybercriminalité ainsi que de la législation sur les preuves électroniques.
Dans cet esprit, permettez-moi de vous souhaiter, au nom de l'Union européenne, des échanges très fructueux et constructifs, avec des résultats concrets pour faire progresser votre législation nationale sur la protection des données et la cybercriminalité, conformément aux normes internationales. Nous restons déterminés à renforcer la coopération avec vous, en particulier dans la phase de mise en œuvre de ces instruments.

Merci de votre attention.