Pour la création d'une cour pénale internationale numérique

Actualité législative publié le **25/01/2025**, vu **67 fois**, Auteur : Yanis MOUHOU

L'essor de l'écosystème des crypto-monnaies, la puissance des échanges numériques, soulève des nouveaux enjeux de criminalité, ainsi que de nouvelles réponses juridiques mondiales.

Introduction

À l’ère de la mondialisation numérique, où les technologies de l'information transforment radicalement nos vies quotidiennes et nos relations internationales, la criminalité numérique émerge comme l'une des menaces les plus redoutables du XXIe siècle. Qu'il s'agisse de cyberattaques massives, de fraudes électroniques, de violations des droits humains en ligne, ou encore de l'exploitation des nouvelles technologies pour commettre des crimes de guerre, le cyberespace est devenu un terrain fertile pour des activités criminelles, souvent transnationales et difficiles à poursuivre. Dans ce contexte, un défi majeur se pose : comment protéger la communauté internationale des dangers du numérique tout en assurant la justice et la responsabilité des auteurs de crimes numériques ? La réponse réside dans la création d’une **Cour Pénale Internationale Numérique (CPIN)**, qui pourrait être un pilier fondamental pour garantir l’ordre et la justice dans le monde numérique.

1. La montée en puissance de la criminalité numérique : un défi mondial

Le phénomène de la criminalité numérique a explosé ces dernières années, couvrant une vaste gamme d'activités criminelles :

- **Les cyberattaques et le cyberterrorisme** : Des groupes criminels ou des États peuvent mener des attaques informatiques visant à paralyser des infrastructures vitales, telles que les réseaux électriques, les systèmes de santé ou les administrations publiques, créant des dommages considérables tant sur le plan économique que sur le plan humain.
- **Les crimes financiers et les fraudes** : Le blanchiment d'argent via les crypto-monnaies, les escroqueries numériques, ou encore le piratage de données personnelles ont pris des proportions inquiétantes, perturbant les économies mondiales.
- **L’exploitation des technologies pour commettre des violations des droits humains** : Le développement de l’intelligence artificielle, de la reconnaissance faciale et des plateformes de surveillance numérique soulève des préoccupations quant à la violation de la vie privée, de la liberté d’expression et d’autres droits fondamentaux. De plus, des crimes de guerre peuvent être perpétrés en ligne, comme la diffusion de propagande violente ou l’incitation à des actes terroristes.
- **Les violations liées à la gouvernance du cyberespace** : Des États ou des acteurs privés

exploitent des plateformes numériques pour mener des actes d’espionnage industriel ou d’ingérence dans des processus électoraux, menaçant ainsi la stabilité politique de nations entières.

Face à l’ampleur de ces défis, il est impératif de créer un mécanisme judiciaire mondial capable de juger les auteurs de crimes numériques, quel que soit leur pays d’origine ou la localisation des victimes.

2. L'inefficacité des systèmes nationaux et internationaux existants

Les systèmes juridiques nationaux, bien qu'efforts louables pour lutter contre la criminalité numérique, sont souvent dépassés par la complexité et la globalité des crimes perpétrés dans le cyberespace. Les raisons principales de cette inefficacité sont les suivantes :

- **L'absence de cadre juridique universel** : Les législations nationales en matière de cybercriminalité sont disparates, ce qui empêche une coopération fluide et efficace entre les États. Il n'existe pas encore de droit pénal international spécifiquement conçu pour la criminalité numérique.
- **Les difficultés liées à la territorialité** : Le cyberespace n’a pas de frontières physiques, ce qui rend difficile l’application de la loi. Un délit commis dans le cyberespace peut être impossible à localiser, et l'identification des responsables est souvent laborieuse.
- **Le manque de ressources et de compétences spécialisées** : Les autorités nationales, notamment dans les pays en développement, manquent souvent de la technologie, des ressources et des compétences nécessaires pour mener des enquêtes complexes sur des cybercrimes à grande échelle.
- **Les limitations des mécanismes internationaux actuels** : Bien que des conventions existent, comme la **Convention de Budapest sur la cybercriminalité** (2001), elles ne sont pas contraignantes pour tous les pays, et leur mise en œuvre reste inégale. De plus, les crimes numériques graves, comme les attaques menées par des États ou les violations massives des droits humains numériques, échappent souvent à toute forme de justice.

3. Pourquoi une Cour Pénale Internationale Numérique ?

3.1 Une réponse à la globalité de la criminalité numérique

La **Cour Pénale Internationale Numérique (CPIN)** serait un tribunal supranational destiné à juger les auteurs de crimes numériques internationaux. Elle répondrait à un besoin pressant de mettre en place une **justice globale** et **transnationale** pour les crimes numériques, qu'ils soient perpétrés par des individus, des groupes criminels, des entreprises ou des États. La CPIN serait dotée de compétences universelles pour poursuivre des actes criminels qui échappent actuellement à la juridiction nationale.

- **Justice pour les victimes de crimes numériques transnationaux** : Beaucoup de victimes de cyberattaques ou de crimes en ligne se trouvent dans des pays où les autorités n’ont ni les moyens, ni la volonté d’engager des poursuites. La CPIN pourrait ainsi garantir la protection des victimes, qu’elles soient des particuliers ou des États.
- **Rendre les auteurs responsables** : Que les criminels numériques soient des acteurs étatiques ou non, la CPIN permettrait de les poursuivre et de les juger de manière indépendante, sans crainte de politisation ou d’ingérence des États.

3.2 Un cadre juridique adapté aux crimes numériques

Une telle cour pourrait compléter les structures existantes comme la **Cour Pénale Internationale (CPI)** ou le **Tribunal Pénal International pour l'ex-Yougoslavie (TPIY)**, en adaptant le droit pénal aux spécificités du cyberespace. Elle pourrait se baser sur des principes de droit international existants, mais les adapter aux enjeux numériques, notamment à travers :

- **L’élargissement de la définition des crimes internationaux** pour y inclure des infractions spécifiques au numérique, comme les cyberattaques contre des infrastructures critiques, le cyberterrorisme, la surveillance illégale ou l’utilisation abusive des technologies de l’information pour violer les droits humains.
- **La création de procédures d'enquête adaptées** pour collecter des preuves numériques, mener des cyber-enquêtes transfrontalières, et assurer la protection des données sensibles et des témoins dans le cyberespace.
- **La mise en place de sanctions adaptées**, non seulement pécuniaires ou pénales, mais aussi des mesures visant à interdire les technologies et les infrastructures utilisées dans le cadre de crimes numériques.

3.3 Une coopération internationale renforcée

La **CPIN** permettrait de renforcer la coopération entre les États membres, notamment en matière de **partage de renseignements** et de **lutte contre l’impunité**. En créant une juridiction mondiale, les gouvernements, les entreprises technologiques et les institutions internationales travailleraient main dans la main pour garantir une gouvernance plus rigoureuse du cyberespace, tout en mettant fin à l'extraterritorialité de certains crimes numériques.

Le succès de cette Cour dépendrait d'un engagement international large, similaire à celui qui a permis la création de la CPI. Une telle institution pourrait également être rendue plus efficace par l'intégration des **partenaires privés**, tels que les entreprises technologiques, qui possèdent des ressources précieuses pour traquer les cybercriminels et sécuriser les réseaux.

4. Les défis à surmonter pour sa création

Bien que l'idée de créer une **Cour Pénale Internationale Numérique** soit séduisante, plusieurs défis restent à surmonter pour sa mise en place :

- **Le manque de consensus international** : Les États doivent s’accorder sur les principes fondamentaux de cette cour, notamment sa compétence, ses procédures, et ses priorités. Certains pays pourraient craindre de perdre leur souveraineté ou leur influence sur le cyberespace.
- **Les problèmes de souveraineté et d'application de la loi** : La question de la **juridiction** se poserait, notamment en cas de crimes commis par des États. Une solution devra être trouvée pour garantir que les nations coopèrent pleinement avec la cour.
- **Les enjeux de financement et de logistique** : Créer et maintenir une cour de cette ampleur nécessiterait des ressources substantielles, à la fois financières et techniques.