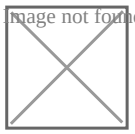

Les nouvelles formes de criminalité

Actualité législative publié le **27/01/2025**, vu **362 fois**, Auteur : Yanis MOUHOU

Les nouvelles formes de criminalité représentent une évolution majeure du paysage criminel mondial.

Introduction

Les **formes de criminalité** ont profondément évolué ces dernières décennies en raison de la montée en puissance des **technologies numériques** et de l'**internet**. Alors qu'auparavant les infractions se limitaient souvent à des actes physiques (vol, meurtre, fraude), l'émergence de nouvelles technologies a engendré des formes de criminalité plus complexes et plus subtiles. Ces nouvelles formes de criminalité incluent notamment la **cybercriminalité**, la **criminalité financière** liée à la technologie, les **crimes numériques** impliquant des **crypto-monnaies**, ainsi que des actes liés à des technologies émergentes telles que **l'intelligence artificielle (IA)** et la **blockchain** .

Cet article se propose d'explorer les **nouvelles formes de criminalité** qui émergent avec l'avancée des technologies numériques, en analysant les défis juridiques associés et les réponses apportées par les États et les régulateurs.

1. La Cybercriminalité : L'Avènement d'un Nouveau Paradigme

a) Les Types de Cybercriminalité

La **cybercriminalité** englobe une large gamme d'infractions qui sont soit facilitées, soit directement commises à l'aide d'outils numériques. Parmi les infractions les plus courantes, on trouve :

- **Le piratage informatique** : l'accès non autorisé à des systèmes informatiques dans le but de voler des données sensibles, de provoquer des dommages ou d'espionner des entreprises ou des États.
- **Les ransomwares** : des logiciels malveillants qui bloquent l'accès à un système informatique ou à des données, avec une demande de paiement en échange de la restauration des données. Ces attaques visent principalement des entreprises, des hôpitaux, des infrastructures critiques, ou des administrations publiques.
- **L'escroquerie en ligne** : des arnaques qui utilisent Internet pour tromper les victimes et les inciter à verser de l'argent ou à fournir des informations personnelles.
- **Le phishing** : une méthode de fraude par laquelle des criminels se font passer pour des entités légitimes pour dérober des informations sensibles telles que des mots de passe, des numéros de carte bancaire ou des identifiants de comptes.

Ces types de crimes sont d'autant plus préoccupants qu'ils peuvent être **transnationaux**, impliquant plusieurs juridictions et rendant leur poursuite difficile. Les attaques par ransomware, par exemple, ne respectent pas les frontières géographiques, ce qui complique leur traitement par les forces de l'ordre.

b) Les Défis Juridiques de la Cybercriminalité

Le principal défi posé par la cybercriminalité est son **caractère transnational**. Un criminel peut se trouver dans un pays, tandis que ses victimes se trouvent dans un autre, ce qui nécessite une **coopération internationale** renforcée pour faire face à cette criminalité. Les **législations nationales** restent souvent limitées par les frontières, et la lutte contre la cybercriminalité exige une coopération juridique entre **les États**, mais aussi avec des **entreprises technologiques** pour lutter efficacement contre les attaques.

De plus, la **vitesse de l'évolution technologique** et des méthodes utilisées par les cybercriminels dépasse souvent la capacité des législateurs à réagir. Le cadre juridique international, bien que renforcé par des initiatives comme la **Convention de Budapest sur la cybercriminalité** de 2001, doit continuellement évoluer pour s'adapter aux nouvelles menaces.

2. La Criminalité Financière Numérique

a) Les Crimes Liés aux Crypto-monnaies

L'apparition des **crypto-monnaies** comme le **Bitcoin**, l'**Ethereum**, et d'autres actifs numériques a donné naissance à de nouvelles formes de criminalité financière. Ces monnaies décentralisées, fondées sur la technologie **blockchain**, présentent des caractéristiques telles que l'anonymat et la décentralisation, qui peuvent être exploitées pour commettre des infractions.

Les **crimes financiers liés aux crypto-monnaies** incluent :

- **Le blanchiment d'argent** : Les transactions anonymes ou semi-anonymes facilitent le **blanchiment d'argent** en permettant aux criminels de dissimuler l'origine de fonds illicites.
- **Le financement du terrorisme** : Les groupes terroristes peuvent utiliser des crypto-monnaies pour **lever des fonds**, les transférer à l'international et financer leurs activités sans être détectés.
- **Les ICO frauduleuses (Initial Coin Offering)** : Certaines entreprises ou individus organisent des ICO pour lever des fonds auprès du public, puis disparaissent avec l'argent collecté. Ce type de fraude est appelé **"exit scam"**.

b) La Régulation des Crypto-monnaies et la Lutte Contre la Criminalité

Les gouvernements ont cherché à adapter leurs **réglementations financières** aux nouvelles réalités des **crypto-monnaies** et de la **blockchain**. Les régulateurs financiers du monde entier ont renforcé leurs efforts pour limiter le **blanchiment d'argent** et le **financement du terrorisme** à travers l'utilisation des crypto-monnaies.

L'**Union européenne** a adopté des règles strictes concernant les **plates-formes d'échange de crypto-monnaies** et impose désormais aux entreprises de respecter les lois anti-blanchiment d'argent (**AML**) et de **connaître leurs clients (KYC)**. De même, les États-Unis ont mis en place des régulations à travers la **Financial Crimes Enforcement Network (FinCEN)** pour surveiller les transactions en crypto-monnaies et empêcher les crimes financiers.

Malgré ces efforts, l'anonymat des transactions et la décentralisation inhérente aux crypto-monnaies rendent difficile leur contrôle complet, soulevant la question de savoir si de nouvelles régulations internationales sont nécessaires pour mieux superviser ce secteur.

3. La Criminalité Associée à l'Intelligence Artificielle (IA) et aux Technologies Emergentes

a) L'IA au service de la Criminalité

L'émergence de l'**intelligence artificielle** a ouvert de nouvelles perspectives dans la criminalité numérique. L'IA peut être utilisée pour créer des **outils de cyber-attaques** automatisés capables de mener des attaques à grande échelle. Par exemple, des **malwares autonomes** qui évoluent et se développent sans intervention humaine peuvent infiltrer des systèmes de manière plus difficilement détectable.

Une autre menace vient des **deepfakes**, une technologie qui permet de créer des vidéos ou des audios totalement réalistes mais fabriqués à l'aide de l'IA. Cette technologie peut être utilisée pour **diffuser de fausses informations**, **tromper** des victimes ou compromettre des élections.

b) Les Défis Juridiques de l'IA et de la Criminalité

L'un des principaux défis juridiques posés par l'IA et les technologies émergentes réside dans leur **difficile réglementation**. Les législations actuelles sont souvent insuffisantes pour appréhender les **nouvelles formes de criminalité** créées par l'IA, en particulier en matière de **protection de la vie privée**, de **propriété intellectuelle** et de **cyber-sécurité**.

Les **lois existantes** sur la **responsabilité pénale** ne sont pas toujours adaptées à des crimes où l'IA joue un rôle central. Par exemple, si un **algorithme** ou un **robot** commet un crime, il devient difficile de déterminer **la responsabilité pénale** (est-ce l'auteur de l'IA, l'utilisateur, ou le créateur de l'algorithme ?). Les législateurs doivent rapidement s'adapter pour définir les contours juridiques de l'**usage de l'IA** et des **techniques émergentes** dans le cadre criminel.

4. Les Cyber-crimes en Évolution : L'Internet des Objets (IoT) et la Criminalité

a) Les risques associés à l'Internet des Objets (IoT)

L'**Internet des Objets** (IoT) permet à une multitude de dispositifs (appareils domestiques, voitures, montres connectées, etc.) d'être reliés à Internet. Cependant, ces dispositifs introduisent des vulnérabilités qui peuvent être exploitées par des cybercriminels. Par exemple, des attaques ciblant des objets connectés peuvent avoir des conséquences dramatiques, comme le piratage de voitures autonomes ou l'intrusion dans des systèmes de santé numériques.

b) La Régulation et la Prévention des Cyber-Crimes liés à l'IoT

À mesure que les appareils IoT se multiplient, les **régulations** devront se concentrer sur la **sécurisation de ces appareils** et la **protection des données** personnelles qu'ils collectent. De nouvelles législations devront être mises en place pour contraindre les fabricants à renforcer la **sécurisation** de leurs produits et à **éduquer les utilisateurs** sur les risques liés à ces nouvelles technologies.