Les nouvelles infractions liées à l'intelligence artificielle

Actualité législative publié le **26/01/2025**, vu **79 fois**, Auteur : Yanis MOUHOU

Ce domaine, est un défi pour le droit pénal dans les années à venir. Il s’agit de garantir la sécurité et l'équité dans un monde où les technologies autonomes jouent un rôle de plus en plus central.

Les nouvelles infractions liées à l'intelligence artificielle : défis juridiques et implications

Introduction

L'intelligence artificielle (IA) transforme de manière profonde et rapide de nombreux secteurs, des industries technologiques à la finance, en passant par la santé, la logistique et même le droit. Cependant, cette évolution technologique soulève des préoccupations croissantes concernant ses implications sur le droit pénal et les comportements criminels. L'IA, en raison de sa capacité à analyser des volumes massifs de données, à prendre des décisions autonomes, et à interagir avec des systèmes complexes, peut être utilisée à des fins malveillantes, engendrant ainsi de nouvelles catégories d'infractions qui nécessitent une réflexion juridique spécifique.

Cet article explore l'émergence de nouvelles infractions pénales liées à l'IA, en analysant leurs aspects juridiques, les défis qu'elles posent, et les approches possibles pour les réguler. Il examine également les risques d'abus technologiques et les manières dont le droit pourrait évoluer pour traiter les comportements criminels associés à l'IA.

I. Les infractions potentielles liées à l'usage malveillant de l'IA

1.1. L’utilisation de l’IA pour commettre des fraudes

L'IA peut être utilisée pour commettre des fraudes sophistiquées en exploitant des systèmes automatisés. Par exemple, des **deepfakes**, ces vidéos manipulées à l’aide de l’IA, peuvent être créées pour diffuser de fausses informations ou pour tromper les victimes dans des contextes de fraude financière, de chantage ou de manipulation politique. Ces deepfakes peuvent également être utilisés pour falsifier des documents ou des preuves dans le cadre d’enquêtes judiciaires, rendant plus complexe la détection de la fraude.

En matière de **cybercriminalité**, les attaquants peuvent utiliser des bots intelligents pour **contourner des systèmes de sécurité**, menant des attaques **DDoS (Distributed Denial of Service)** ou de **phishing**. De plus, l'IA peut être utilisée pour automatiser des processus de fraude fiscale, en manipulant les systèmes de déclaration ou en utilisant des logiciels pour escroquer des informations sensibles.

Juridiquement, la question se pose de savoir si des infractions commises par des IA peuvent être traitées avec les mêmes principes que celles commises par des individus humains. Peut-on tenir l'IA responsable d'un délit, ou faut-il remonter à la responsabilité des concepteurs ou utilisateurs de l'IA ? Ces questions sont au cœur des débats juridiques.

1.2. L'IA dans la manipulation des marchés

Les **algorithmes de trading** utilisant l'IA sont de plus en plus populaires dans le secteur financier. Cependant, ces algorithmes peuvent être utilisés pour manipuler les marchés en effectuant des **transactions automatisées** qui créent des fluctuations artificielles de prix. Les techniques telles que le **"spoofing"**, où un trader place des ordres de vente ou d'achat qu'il n'a pas l'intention d'exécuter, peuvent être automatisées par des systèmes intelligents pour manipuler les valeurs boursières.

Les autorités de régulation financière, telles que la **SEC** (Securities and Exchange Commission) aux États-Unis ou l'**ESMA** (European Securities and Markets Authority) en Europe, surveillent de près ces pratiques, mais le droit actuel peine à s'adapter à ces nouvelles technologies. Une question centrale est de savoir dans quelle mesure les régulations existantes, comme celles encadrant les marchés financiers, peuvent être appliquées à des transactions automatisées opérées par des IA.

1.3. L'IA et les risques de discrimination algorithmique

Une autre infraction émergente liée à l'IA concerne la **discrimination algorithmique**, lorsqu'un système d'IA prend des décisions biaisées ou injustes à l'encontre de certaines populations. Cela peut se manifester dans des domaines tels que l'embauche, les prêts bancaires, l'octroi de crédits, ou même les décisions judiciaires, où l'IA est utilisée pour évaluer les risques ou effectuer des prédictions.

Les **discriminations raciales, de genre ou socio-économiques** peuvent être exacerbées par l'usage de l'IA si les données d'entraînement sont biaisées. Par exemple, un algorithme de recrutement pourrait, par inadvertance, favoriser les candidats masculins en raison de biais dans les données historiques d'embauche. Bien que ces discriminations ne relèvent pas directement d'un comportement malveillant, elles peuvent tout de même constituer une forme d'**injustice systématique** qui pourrait être considérée comme une infraction sous le droit pénal.

En réponse à ce phénomène, plusieurs juridictions envisagent des régulations pour encadrer l'utilisation des IA, notamment en matière de **transparence des algorithmes**, **d'audit indépendant** et de **droit de recours** pour les personnes affectées par des décisions discriminatoires prises par des intelligences artificielles.

II. Les défis juridiques posés par les infractions liées à l'IA

2.1. La responsabilité pénale des IA : qui est responsable ?

L'un des défis juridiques majeurs en matière d'infractions liées à l'IA est la question de la **responsabilité pénale**. Actuellement, le droit pénal repose sur le principe selon lequel une personne humaine peut être tenue responsable d'une infraction. Toutefois, lorsqu'une IA commet une infraction, il est difficile d'attribuer cette responsabilité à la machine elle-même, qui ne dispose pas de personnalité juridique.

Les infractions commises par des IA soulèvent donc la question de la **responsabilité des concepteurs, des utilisateurs, et des développeurs**. Peut-on imputer la faute à ceux qui ont programmé l'IA, ou à ceux qui l'ont utilisée ? Dans certains cas, des **responsabilités partagées** pourraient être envisagées, où les acteurs humains sont tenus responsables des actions de leurs machines, notamment en cas de négligence dans la programmation ou l'utilisation d'une IA.

2.2. La question de la régulation des IA : un cadre juridique en construction

Les législations actuelles peinent à suivre l'évolution rapide des technologies d'IA. Les régulations sont souvent générales et ne prévoient pas des normes spécifiques adaptées aux spécificités de l'IA et de ses usages criminels. La régulation des IA dans le contexte des infractions pénales devra probablement passer par deux axes :

1. **Une régulation technique** visant à encadrer les risques que l'IA présente pour la sécurité publique, économique et sociale. Cela inclut la création de normes pour l'audit des algorithmes, la certification des IA en fonction de critères de sécurité et de non-discrimination, et la mise en place de contrôles pour éviter les abus.

2. **Une régulation pénale** spécifiquement dédiée à la gestion des infractions liées à l'IA. Il sera nécessaire de créer des infractions pénales spécifiques pour les crimes commis par des IA, notamment en matière de fraude, de manipulation des marchés, et de discrimination. Les législateurs devront aussi définir des **sanctions adaptées** à la fois pour les responsables humains et pour les entités juridiques qui mettent en œuvre des systèmes d'IA délictueux.

2.3. La sécurité des IA : prévenir les abus

L'un des risques majeurs est l'utilisation de l'IA pour des fins malveillantes, comme le piratage, les attaques sur des infrastructures critiques, ou la manipulation de données sensibles. Les IA peuvent être utilisées pour **contourner des systèmes de sécurité**, comme les **firewalls** ou les **systèmes de détection de fraudes**, ou même pour conduire des attaques **cybercriminelles** en analysant des vulnérabilités dans des systèmes complexes.

La sécurité des IA elle-même doit donc être au cœur des préoccupations. Des infractions pénales pourraient être envisagées pour les développeurs d'IA qui ne respectent pas les normes de sécurité, ou pour les utilisateurs d'IA qui permettent à leurs systèmes d'être utilisés à des fins criminelles. Un cadre juridique spécifique pour la **protection des IA** contre les abus et les piratages pourrait émerger pour prévenir ce type de risques.

III. Les solutions possibles : un cadre juridique dynamique

3.1. L'émergence de normes internationales

Face à l'internationalisation des réseaux et des technologies d'IA, les infractions liées à l'IA nécessitent un cadre juridique mondial. La **Commission européenne** a déjà proposé un projet de règlement sur l'intelligence artificielle qui vise à établir des **normes de sécurité**, de **transparence** et de **non-discrimination**. Un tel modèle pourrait inspirer d'autres pays à adopter des normes similaires, créant ainsi un **consensus mondial** sur la gestion des risques associés à l'IA.

3.2. La responsabilisation des acteurs humains

Une approche clé pour résoudre les questions de responsabilité pourrait être de **renforcer la responsabilisation des acteurs humains** impliqués dans l'utilisation des IA. Cela pourrait inclure des exigences de transparence dans la conception des systèmes, des obligations de surveillance continue et d'audit des IA, ainsi que la mise en place de sanctions pour ceux qui ne respectent pas ces obligations.