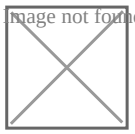

De la criminalité dans le métavers

Actualité législative publié le **25/01/2025**, vu **104 fois**, Auteur : Yanis MOUHOU

Le développement du métavers soulève des nouveaux enjeux en matière de criminalité et de réponse pénale. Cet article évoque ce sujet contemporain.

La criminalité dans le métavers : défis, risques et réponses juridiques

Introduction

Le métavers, univers virtuel en pleine expansion, suscite de nombreuses attentes, notamment en termes de révolution numérique, mais aussi d'interactions sociales, économiques et culturelles. En parallèle, son développement rapide expose les utilisateurs à des risques nouveaux en matière de criminalité, soulignant la nécessité de réguler ces espaces pour protéger les participants. Si le métavers est vu comme un nouvel Eldorado technologique, il est également un terrain fertile pour des comportements criminels, tels que les escroqueries numériques, le harcèlement en ligne, la fraude, ou le piratage informatique. Cet article explore les diverses formes de criminalité dans le métavers, les défis juridiques qu'elles suscitent, et les réponses légales envisageables pour encadrer cet espace virtuel.

1. Définition du métavers et caractéristiques clés

Le métavers désigne un univers numérique immersif où les utilisateurs peuvent interagir entre eux, participer à des activités économiques, sociales et culturelles, ou encore interagir avec des objets numériques. Il combine principalement la réalité virtuelle (VR) et la réalité augmentée (AR), mais repose aussi sur des systèmes basés sur la blockchain et les crypto-monnaies, ce qui permet des transactions économiques décentralisées.

Parmi ses caractéristiques majeures, on peut citer :

- **L'immersion** : Le métavers est conçu pour une expérience immersive, où les utilisateurs sont représentés sous forme d'avatars, interagissant avec des environnements 3D.
- **L'interactivité** : L'utilisateur est acteur dans ce monde numérique, pouvant influencer l'environnement virtuel et interagir avec d'autres participants en temps réel.
- **L’économie virtuelle** : Le métavers repose sur une économie numérique où les utilisateurs peuvent acheter, vendre ou échanger des biens virtuels via des monnaies numériques, des NFT (tokens non fongibles), ou des actifs numériques.

Toutefois, la décentralisation et l'anonymat du métavers, couplés à la forte interconnexion des plateformes virtuelles, posent de nouveaux défis pour la régulation et la protection juridique des utilisateurs.

2. Les formes de criminalité dans le métavers

2.1 Fraude et escroquerie numérique

L'une des premières formes de criminalité dans le métavers concerne les **escroqueries numériques**. Ces actes incluent les fraudes liées aux achats de biens virtuels inexistants ou contrefaits, ainsi que des arnaques impliquant des NFTs, des crypto-monnaies, ou des plateformes de jeu.

- **Phishing et scams** : Des criminels peuvent inciter les utilisateurs à entrer des informations personnelles, telles que des clés privées de portefeuilles de crypto-monnaies, ou à transférer des fonds via des plateformes frauduleuses, leur permettant ainsi de voler leurs actifs numériques.
- **Vente de NFTs contrefaits** : Le marché des NFTs, qui repose sur la technologie blockchain, est souvent la cible de fraudeurs qui créent de faux NFT et les vendent à des prix exorbitants.

L'**article 313-1 du Code pénal français** définit la fraude comme l'utilisation de moyens malhonnêtes pour induire une personne en erreur dans le but de lui soutirer un bien ou un service. Dans le cadre du métavers, cette même définition pourrait s'appliquer aux transactions frauduleuses impliquant des biens virtuels, ce qui pose un défi majeur en matière de juridiction et de preuves.

L'article 313-1 du Code pénal dispose :

> *"L'escroquerie est le fait, par l'usage de manœuvres frauduleuses, d'amener une personne à remettre des fonds, des biens ou à consentir un acte juridique au détriment de ses intérêts."*

Les escroqueries numériques dans le métavers peuvent donc être poursuivies sur cette base juridique, mais l'exécution effective de ces poursuites dépendra de la juridiction et de la nature transnationale des plateformes concernées.

2.2 Harcèlement et comportements abusifs

Le harcèlement dans le métavers, également connu sous le nom de **"griefing"**, implique des actes de nuisance ou d'abus physiques ou psychologiques à l'encontre des autres utilisateurs. Ce phénomène peut se traduire par des agressions verbales, des insultes, du harcèlement sexuel ou des comportements de type cyberbullying, qui sont amplifiés par l'immersion dans un environnement virtuel.

- **Harcèlement sexuel et comportement abusif** : Dans certaines plateformes du métavers, des utilisateurs peuvent harceler d'autres en utilisant des avatars ou en envoyant des messages inappropriés, parfois accompagnés de contenus ou de comportements visuels perturbants.
- **Violence virtuelle** : Des avatars peuvent être utilisés pour poursuivre d'autres utilisateurs, violer leur espace privé ou perturber leur expérience.

L'**article 222-33 du Code pénal français** réprime le harcèlement moral ou sexuel, qu'il soit commis dans un environnement physique ou numérique :

"Le harcèlement moral est constitué par des agissements répétés qui ont pour effet de porter atteinte à la dignité de la personne, ou de créer à son égard une situation intimidante, hostile, dégradante, humiliante ou offensante."

Le cadre législatif français permet de poursuivre les auteurs de harcèlement dans le métavers sous cette qualification, bien que la difficulté réside dans l'identification de l'auteur et la preuve des faits.

2.3 Trafic de biens et substances illicites

Le métavers peut également faciliter des activités criminelles physiques, comme le **trafic de biens et de substances illicites**. Par exemple, des objets virtuels pourraient être utilisés pour simuler des échanges de substances illégales, de drogues ou d'armes, ou bien pour faciliter des transactions illégales dans le monde réel.

- **Monnaies numériques et blanchiment d'argent** : Le recours à des **cryptomonnaies** et à des **NFTs** rend le traçage des transactions financières plus complexe. Ces outils numériques sont parfois utilisés pour le blanchiment d'argent ou le financement d'activités illégales, ce qui constitue un risque majeur pour les autorités fiscales et judiciaires.

Le **Code pénal français, article 324-1**, punit le blanchiment de fonds illicites :

"Le blanchiment de fonds est constitué par le fait de dissimuler ou de transformer l'origine illicite d'une ressource ou d'un bien, en particulier par la conversion ou le transfert de ces ressources dans le but de les rendre légitimes."

Cela inclut le blanchiment via des plateformes de cryptomonnaies ou des échanges de biens virtuels dans le métavers, bien que la difficulté réside dans la traçabilité des actifs numériques et leur attribution à un individu physique.

2.4 Piratage informatique et cybercriminalité

Le piratage informatique dans le métavers est un phénomène croissant, particulièrement en raison de la valeur marchande des actifs numériques (NFTs, crypto-monnaies). Les cybercriminels peuvent exploiter des vulnérabilités dans les plateformes pour accéder à des **portefeuilles numériques** et voler des biens virtuels.

- **Piratage de comptes utilisateurs** : Les attaques peuvent inclure le vol d'identifiants d'utilisateur, la manipulation de portefeuilles numériques, ou l'infiltration des **smart contracts** pour dérober des fonds.

L'**article 323-1 du Code pénal** définit le piratage informatique comme un crime :

"Le fait d'accéder, de manière frauduleuse, à tout ou partie d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende."

Cette définition peut être appliquée au piratage d’une plateforme de métavers, notamment lorsqu’un hacker accède à un portefeuille numérique ou à des informations privées liées à un utilisateur.

3. Les défis juridiques posés par la criminalité dans le métavers

3.1 Juridiction et gouvernance

Le **problème de la juridiction** est central dans le métavers. En raison de son absence de frontières physiques, un crime peut être commis dans un environnement virtuel tout en impliquant plusieurs juridictions. Les plateformes virtuelles peuvent être hébergées dans un pays, tandis que les victimes ou les criminels sont situés dans d'autres, rendant la régulation complexe.

La **régulation transnationale** semble indispensable, en particulier pour encadrer les crimes transfrontaliers comme le blanchiment d’argent ou le trafic de biens illicites. À cet égard, des accords internationaux doivent être mis en place pour établir des règles communes sur les droits et obligations des utilisateurs dans le métavers.

Le **règlement (UE) n° 910/2014 relatif à l'identification des utilisateurs dans les systèmes de paiement** (règlement sur l’identification des clients) pourrait servir de modèle pour instaurer des normes similaires dans le métavers.

3.2 Anonymat et décentralisation

L'anonymat est une caractéristique clé du métavers, facilité par l’utilisation de **pseudonymes** et de **cryptomonnaies**. Cet anonymat, tout en protégeant la vie privée des utilisateurs, constitue également un obstacle majeur pour les autorités judiciaires qui tentent d’identifier et de poursuivre les criminels. La décentralisation des plateformes – notamment les **plateformes basées sur la blockchain** – complique encore la tâche des régulateurs, car elles échappent souvent à l'autorité d'une entité centrale.

Le recours aux **crypto-monnaies anonymes** comme Monero ou Zcash constitue un obstacle supplémentaire pour le suivi des flux financiers suspects. Les autorités devront mettre en place des **technologies de traçabilité**, afin de rendre ces transactions plus transparentes, tout en respectant la vie privée des utilisateurs.

3.3 Protection des données personnelles

Le **règlement général sur la protection des données (RGPD)** de l'Union européenne et d'autres législations de protection des données seront cruciales pour encadrer les activités du métavers, où de grandes quantités de données personnelles sont collectées et échangées. Ces données peuvent être utilisées à des fins commerciales ou, dans le pire des cas, être exploitées par des criminels.

4. Réponses juridiques possibles

4.1 Législation et régulation internationale

Afin de limiter la criminalité dans le métavers, une **législation internationale** spécifique est essentielle. L'unification des lois à travers des conventions mondiales pourrait constituer une base

juridique pour la régulation des comportements criminels dans les mondes virtuels.

4.2 Création de règles éthiques et modération

Les plateformes de métavers doivent adopter des **codes de conduite stricts** et des mécanismes de modération active. Cela inclut la mise en place de **systèmes de reporting** efficaces et de **sanctions** pour les utilisateurs qui enfreignent les règles, notamment en matière de harcèlement, de fraude ou de piratage.

4.3 Collaboration entre acteurs privés et autorités publiques

La coopération entre les **autorités publiques**, telles que les autorités de régulation financière et les **forces de l’ordre**, et les acteurs privés (développeurs, plateformes de jeux, entreprises de cryptomonnaies) est cruciale pour mettre en place des systèmes de surveillance et de prévention efficaces.