NFT et criminalité internationale

Actualité législative publié le **27/01/2025**, vu **112 fois**, Auteur : Yanis MOUHOU

De la fraude et des escroqueries aux violations des droits d'auteur et au blanchiment d'argent, ces actifs numériques sont exploités parfois à des fins illicites.

Depuis leur apparition, les **tokens non fongibles (NFTs)** ont attiré une attention considérable en raison de leur capacité à révolutionner le marché de l'art, des objets de collection et des biens numériques. Cependant, derrière leur potentiel d'innovation se cache également un terrain fertile pour diverses activités criminelles. De la fraude à la **blanchiment d'argent** en passant par des **escroqueries** liées à des **rug pulls** et des **attaques de phishing**, les **NFTs** sont rapidement devenus un vecteur d'activités illicites. Dans cet article, nous explorerons les liens entre **NFTs** et criminalité, les défis juridiques qu'ils posent, et les réponses apportées par les autorités réglementaires.

1. Les NFTs : Une Technologie Révolutionnaire à Double Tranchant

Les **NFTs** sont des unités de données cryptographiques uniques enregistrées sur une **blockchain** , principalement sur des plateformes comme **Ethereum**, **Solana**, ou **Polygon**. Ces actifs numériques ont la particularité de ne pas être interchangeables, contrairement aux **cryptomonnaies** comme le Bitcoin ou l'Ethereum. Les NFTs peuvent représenter une variété de contenus numériques tels que des œuvres d'art, des musiques, des vidéos, des éléments de jeux vidéo, voire des titres de propriété numérique.

Cette capacité à certifier l'unicité d'un objet numérique en a fait un produit prisé dans des secteurs comme l'art, les jeux vidéo et la mode. Toutefois, cette unicité et cette traçabilité en font également une cible de choix pour diverses formes de criminalité, en raison de la décentralisation et de l'anonymat partiel qu'offrent les plateformes de **blockchain**.

2. Les NFTs et les Formes de Criminalité

a. Fraude et Escroqueries : Les Rug Pulls

L'une des formes de criminalité les plus courantes dans l'écosystème des NFTs est le phénomène des **rug pulls**. Ce terme désigne une **escroquerie** dans laquelle un développeur ou un groupe de créateurs d'un projet NFT attire des investisseurs, souvent en promettant des rendements rapides ou des produits exclusifs, puis disparaît avec les fonds sans livrer les biens promis.

Les rug pulls exploitent souvent la **spéculation** et la **manque de régulation** dans l'écosystème des NFTs, où des projets peuvent être lancés rapidement, sans transparence ni responsabilité. Ces arnaques peuvent aussi inclure des **faux comptes** ou des **collections contrefaites**, où les créateurs volent l'identité d'artistes célèbres ou de marques pour créer des NFTs illégaux et les

vendre à des prix exorbitants.

b. Blanchiment d'Argent via les NFTs

Les **NFTs** offrent un moyen potentiellement efficace de **blanchir de l'argent** en raison de leur marché peu surveillé et de l'absence de régulations uniformes. Les criminels peuvent acheter des NFTs avec des fonds provenant de **transactions illicites** (drogues, financement du terrorisme, etc.), puis revendre ces actifs numériques à des prix gonflés ou les transférer à travers différentes wallets ou plateformes, dissimulant ainsi l'origine des fonds.

Le processus de blanchiment peut se faire de plusieurs manières :

- **Achats et ventes circulaires** : Un même NFT est vendu entre différents comptes contrôlés par les mêmes personnes, créant l'illusion d'une demande et d'une légitimité de valeur.
- **Transferts entre des wallets anonymes** : L'utilisation de plusieurs portefeuilles peut rendre la traçabilité des fonds difficile, voire impossible.
- **Conversion en cryptomonnaies** : Après avoir obtenu des NFTs via des fonds illicites, les criminels peuvent convertir ces actifs en cryptomonnaies, qui peuvent ensuite être échangées sur des plateformes d'échange de crypto-actifs, offrant une couche supplémentaire de dissimulation.

c. Hacking et Phishing pour Voler des NFTs

Le hacking et le phishing sont également des techniques couramment utilisées pour voler des NFTs. Les victimes peuvent être ciblées par des attaques de phishing où les hackers imitent des plateformes populaires de NFTs, comme **OpenSea** ou **Rarible**, pour collecter des informations de connexion et des clés privées. Une fois les informations récupérées, les criminels peuvent accéder aux portefeuilles des victimes et voler leurs NFTs.

Ces attaques se sont intensifiées, notamment lors de l'augmentation des prix des NFTs, avec des plateformes et des portefeuilles devenus des cibles privilégiées. Certains pirates informatiques ont aussi utilisé des **exploits de contrats intelligents** pour manipuler des transactions et récupérer des NFTs ou des fonds d’utilisateurs.

d. Contrefaçon d'Œuvres d'Art Numériques et Piratage de Propriétés Intellectuelles

Un autre type de criminalité concerne la **contrefaçon d'œuvres d'art numériques** sous forme de NFTs. Dans ce cas, des individus créent des NFTs à partir d'œuvres d'art ou de créations numériques protégées par des droits d'auteur, sans l'autorisation des créateurs originaux. Cette contrefaçon numérique, souvent appelée **NFT Piracy**, permet à des criminels de vendre des œuvres qu’ils n'ont pas créées et de s'approprier l'argent sans en reverser une partie aux véritables auteurs.

Cette forme de piratage pose de graves questions en matière de propriété intellectuelle, car la blockchain permet de prouver la vente de ces œuvres contrefaites, créant une situation complexe pour les artistes originaux souhaitant protéger leurs créations.

3. Les Réponses Juridiques et Réglementaires Face à la Criminalité des NFTs

La criminalité liée aux NFTs soulève plusieurs défis pour les régulateurs et les autorités judiciaires. En raison de leur nature décentralisée et souvent anonyme, les NFTs échappent à un cadre

juridique clair et cohérent. Cependant, plusieurs mesures et approches ont été mises en place pour tenter de lutter contre les activités criminelles associées aux NFTs.

a. Législation et Règlementation Nationale

Certains pays ont déjà pris des mesures pour réglementer l'utilisation des NFTs, principalement dans le cadre de la **lutte contre le blanchiment d'argent (AML)** et la **connaissance du client (KYC)**. Par exemple, aux États-Unis, la **Financial Crimes Enforcement Network (FinCEN)** a imposé des exigences aux plateformes d'échange de crypto-actifs qui pourraient aussi s'appliquer aux places de marché NFT, exigeant des vérifications d'identité et des rapports sur les transactions suspectes.

En France, l'**Autorité des Marchés Financiers (AMF)** a publié des orientations concernant les ICOs (Initial Coin Offerings) et a exprimé un intérêt croissant pour la régulation des NFTs, en particulier en ce qui concerne la protection des investisseurs et des droits de propriété intellectuelle.

b. Initiatives Européennes et Globales

Au niveau européen, la **Commission européenne** a reconnu les NFTs comme une catégorie de **crypto-actifs** et a proposé une législation afin d'encadrer les **transactions sur les marchés numériques**. Le **Règlement MiCA (Markets in Crypto-Assets)**, en cours d'élaboration, pourrait étendre les règles AML/KYC aux plateformes de NFTs, en veillant à protéger les consommateurs et à assurer la transparence des transactions.

La **Financial Action Task Force (FATF)**, organisation internationale chargée de la lutte contre le blanchiment d'argent et le financement du terrorisme, a recommandé des lignes directrices pour réguler le marché des crypto-actifs, incluant les NFTs. Bien que la FATF ne dispose pas de pouvoir d'imposition directe, ses recommandations influencent de nombreux pays dans leur approche législative.

c. Sécurisation des Plateformes et Responsabilisation des Acteurs du Marché

Certaines plateformes de **marché NFT**, comme **OpenSea** et **Rarible**, ont commencé à renforcer leurs mesures de sécurité et à mettre en place des procédures de vérification des œuvres proposées à la vente. Ces plateformes tentent également d'appliquer des protocoles de **lutte contre la fraude** et d'identifier les comptes suspects. Cela pourrait inclure des systèmes d'alerte, une vérification des identités des créateurs de NFTs et une lutte contre la vente de contrefaçons.

d. Défis de Mise en Œuvre et Solutions à Long Terme

Les autorités sont confrontées à un grand défi pour traquer les **actes criminels** associés aux NFTs, car les transactions sont effectuées via des **portefeuilles anonymes** et les plateformes de NFT sont souvent peu régulées. À l'avenir, un système de certification et de traçabilité des transactions pourrait être instauré, combiné à un **système de notation** des créateurs de NFTs pour éviter les fraudeurs.