



Crypto-monnaies et financement du terrorisme

Actualité législative publié le 26/01/2025, vu 210 fois, Auteur : [Yanis MOUHOU](#)

La coopération internationale, la mise en place de réglementations efficaces, et le développement de technologies de traçabilité sont des éléments clés dans la lutte contre le financement du terrorisme.

Le **financement du terrorisme** est un défi mondial majeur, et avec l'émergence des **crypto-monnaies**, de nouvelles avenues pour les acteurs malveillants ont été ouvertes. Alors que les **crypto-monnaies** offrent une grande promesse d'inclusivité et de décentralisation, elles représentent également un **risque accru** en matière de financement illicite, y compris le financement du terrorisme.

Les **caractéristiques des crypto-monnaies**, comme la **transparence** des transactions (sur certaines blockchains), l'**anonymat relatif** et la possibilité de réaliser des transactions transfrontalières rapides, facilitent des activités financières difficiles à tracer. Cela permet à des **groupes terroristes** ou à des **individus** sous sanctions de contourner les systèmes financiers traditionnels, échappant ainsi aux contrôles réglementaires classiques.

Cet article pourrait aborder les questions suivantes :

- **La facilitation du financement du terrorisme via les crypto-monnaies** : Comment les **terroristes** et autres groupes criminels utilisent-ils les crypto-monnaies pour transférer de l'argent de manière discrète et décentralisée ? Quels sont les types de **transactions suspectes** les plus courants ?
- **Les efforts de régulation internationale** : Comment les gouvernements et les régulateurs internationaux (comme le **FATF** – Groupe d'Action Financière) cherchent-ils à surveiller les transactions en crypto-monnaies ? Quels mécanismes existent pour **suivre et interdire** les flux financiers liés à des activités terroristes, et comment peuvent-ils être améliorés ?
-

Les outils de traçabilité et de régulation : Quelles technologies existent pour **suivre les transactions en crypto-monnaies** et identifier les acteurs impliqués dans des financements illégaux ? Le rôle des "**crypto-forensics**" (analyses forensiques des crypto-monnaies) dans la détection de ces activités.

- **Les limites et défis de la régulation** : Bien que la **blockchain** soit transparente, le **anonymat** de certaines crypto-monnaies (par exemple, **Monero** ou **Zcash**) complique grandement les efforts de traçabilité. Comment les régulations peuvent-elles **équilibrer** la lutte contre le financement du terrorisme et l'innovation dans l'espace crypto ?
- **L'impact sur la vie privée des utilisateurs** : Comment protéger l'anonymat des utilisateurs légitimes de crypto-monnaies tout en luttant contre les abus ? La question de la **surveillance excessive** des transactions en crypto-monnaies pourrait entraîner des débats sur la protection des **libertés individuelles**.

Ce sujet soulève des **enjeux juridiques** complexes, mêlant **sécurité internationale**, **protection de la vie privée** et **régulation de l'innovation**. Alors que certains plaident pour des restrictions sévères sur les crypto-monnaies pour lutter contre le financement du terrorisme, d'autres s'inquiètent des **répercussions négatives** de telles régulations sur l'**innovation** et la **liberté économique**.

En somme, la lutte contre le **financement du terrorisme** et l'usage des crypto-monnaies comme **outil financier décentralisé** forme un terrain de réflexion et de débat passionnant, avec des répercussions profondes pour la **régulation internationale** et les **droits fondamentaux**. C'est un sujet qui représente un véritable **défi juridique**, à l'intersection de la **technologie**, de la **sécurité** et des **libertés civiles**.

Vous avez dit :

ecrit moi un article juridique precis et approfondi sur les crypto et le financement du terrorisme

ChatGPT a dit :

ChatGPT

Crypto-monnaies et Financement du Terrorisme : Enjeux Juridiques et Régulations

Le financement du terrorisme est un enjeu mondial majeur qui a profondément impacté la manière dont les systèmes financiers sont régulés. L'émergence des **crypto-monnaies** a ajouté une couche supplémentaire de complexité à ce problème, en permettant des transactions financières transfrontalières rapides, souvent anonymes, et en échappant aux dispositifs traditionnels de surveillance financière. Cet article explore les défis juridiques liés à l'utilisation des crypto-monnaies pour le financement du terrorisme et les mesures prises par les régulateurs pour contrer

cette menace.

1. L'Essence du Financement du Terrorisme et les Crypto-monnaies

Le **financement du terrorisme** désigne l'acte de fournir des fonds à des individus ou des groupes dans le but de soutenir des actes terroristes. Traditionnellement, ces financements provenaient de sources diverses, telles que des dons, des taxes imposées dans certaines régions, ou encore des trafics illégaux. Cependant, avec l'essor des crypto-monnaies, des groupes terroristes ont trouvé un moyen d'accéder à des fonds de manière discrète, rapide et souvent sans la surveillance des institutions financières traditionnelles.

Les **crypto-monnaies** telles que **Bitcoin**, **Ethereum**, et d'autres actifs numériques ont été utilisées pour envoyer des fonds à travers les frontières sans l'intermédiaire de banques ou d'autres institutions financières centralisées. Bien que les **blockchains** soient transparentes, les crypto-monnaies offrent souvent un **anonymat relatif**. Les transactions peuvent être réalisées de manière pseudonyme, ce qui les rend difficiles à tracer pour les autorités de régulation. Certaines monnaies numériques, comme **Monero** et **Zcash**, ont été spécifiquement conçues pour **garantir l'anonymat** total des transactions, ce qui les rend encore plus attractives pour des activités illégales, y compris le financement du terrorisme.

2. Les Risques Associés à l'Utilisation des Crypto-monnaies pour le Financement du Terrorisme

L'utilisation des crypto-monnaies pour financer des activités terroristes présente plusieurs risques pour les autorités de régulation et de sécurité :

- **Anonymat et Décentralisation** : Bien que certaines blockchains publiques comme Bitcoin soient transparentes, leur nature **décentralisée** et **pseudo-anonyme** peut rendre l'identification des acteurs malveillants extrêmement difficile. Par ailleurs, l'usage de portefeuilles cryptographiques multiples et de services de **mixing** (mélange de transactions pour rendre les fonds non traçables) complique davantage les efforts de traçabilité.
- **Transactions Transfrontalières** : Les crypto-monnaies permettent de réaliser des transactions instantanées et sans frontières, ce qui est particulièrement avantageux pour les groupes terroristes opérant à l'échelle mondiale. Ces transactions peuvent contourner les lois nationales sur le contrôle des flux financiers, ce qui constitue un défi pour les autorités de surveillance.
- **Évasion des Sanctions** : Les groupes terroristes et les acteurs associés peuvent contourner les sanctions économiques internationales en utilisant les crypto-monnaies pour effectuer des paiements ou financer des opérations, évitant ainsi les **mesures de gel d'avoirs** traditionnelles mises en place par les États et les organisations internationales.

3. Les Réponses Juridiques et Réglementaires

Les régulateurs du monde entier ont pris conscience des dangers posés par l'utilisation des crypto-monnaies dans le financement du terrorisme. Plusieurs initiatives ont été mises en place pour

tenter de répondre à ces défis.

3.1. L'Approche Internationale : Le Rôle du GAFI

Le **Groupe d'Action Financière (GAFI)**, un organisme international de régulation, a adopté des lignes directrices spécifiques concernant l'usage des crypto-monnaies dans le cadre de la lutte contre le blanchiment d'argent et le financement du terrorisme. Dans ses **Recommandations** révisées en 2019, le GAFI a appelé les pays à réguler les **fournisseurs de services d'actifs virtuels (VASP)** et à imposer des obligations de **due diligence** (vérification de l'identité des clients), telles que celles imposées aux institutions financières traditionnelles.

Les crypto-échanges, les **portefeuilles numériques**, et les **fournisseurs de services d'actifs numériques** (tels que les plateformes de trading de crypto-monnaies) doivent désormais collecter des informations sur leurs utilisateurs, telles que l'identité des bénéficiaires et les **transmissions de fonds**, dans le but de lutter contre les activités illégales, y compris le financement du terrorisme.

3.2. Les Régulations Européennes : L'Enforcement du Règlement MiCA et la 5e Directive AML

Au niveau européen, la lutte contre le financement du terrorisme lié aux crypto-monnaies est régie par plusieurs régulations, dont la **Directive européenne anti-blanchiment (5AMLD)**. Cette directive impose aux plateformes de trading de crypto-monnaies des **obligations de KYC** (Know Your Customer) et de **lutte contre le blanchiment d'argent (AML)**. Elle exige également que ces plateformes **identifient et surveillent** les transactions suspectes, notamment celles qui pourraient être liées au financement du terrorisme.

Par ailleurs, le projet de **règlement MiCA (Markets in Crypto-assets)**, en cours de discussion, vise à établir un cadre plus détaillé pour la régulation des crypto-monnaies et des services associés en Europe. MiCA entend renforcer les mesures de **surveillance des transactions** et garantir une plus grande **sécurité** pour les investisseurs tout en limitant les risques associés aux transactions en crypto-monnaies.

3.3. Les Efforts aux États-Unis : L'Approche de la SEC et du FinCEN

Aux États-Unis, la **Securities and Exchange Commission (SEC)** et le **Financial Crimes Enforcement Network (FinCEN)** jouent un rôle central dans la régulation des crypto-monnaies. Le FinCEN impose des obligations aux entreprises de crypto-monnaies, telles que le **déclaration de transactions suspectes** et le **respect des lois anti-blanchiment**. Les entreprises doivent également se conformer à des normes strictes en matière de **KYC** et de **reporting** pour éviter que leurs services ne soient utilisés à des fins de financement du terrorisme.

Les régulations américaines imposent également des restrictions sévères sur les **transactions anonymes**. Les plateformes doivent signaler toute activité suspecte ou anormale, y compris celles impliquant des **groupes terroristes connus**.

4. Défis et Perspectives

Malgré ces efforts de régulation, plusieurs défis demeurent. Le principal est la nature décentralisée des crypto-monnaies, qui empêche une régulation centralisée et impose aux autorités de régulation de développer des techniques de **traçabilité plus avancées**. De plus, le **privacy coin** (monnaies de confidentialité) comme **Monero** et **Zcash** continuent de poser des

obstacles considérables à l'identification des transactions suspectes.

Enfin, une question fondamentale réside dans l'équilibre à maintenir entre **protéger la liberté individuelle** des utilisateurs de crypto-monnaies et **empêcher les abus** qui peuvent nuire à la sécurité mondiale. Les régulations doivent être **flexibles** pour ne pas nuire à l'innovation tout en étant suffisamment strictes pour empêcher l'utilisation des crypto-monnaies à des fins criminelles.