AIX-MARSEILLE UNIVERSITÉ

FACULTÉ DE DROIT ET DE SCIENCE POLITIQUE

MASTER 2 « SÉCURITÉ INTÉRIEURE »

LA CRIMINALITÉ 3.0: ENJEUX ET PERSPECTIVES DE LUTTE FACE AU DÉVELOPPEMENT DE LA BLOCKCHAIN

Présenté et soutenu par

FRANCHINI MAXIME

Directrice de recherche: Madame Frédérique CHOPIN, MCF HDR en droit privé, CDS, AMU

- Année 2022 / 2023 -

« La Faculté n’entend donner ni approbation ni improbation aux opinions émises dans ce mémoire, qui doivent être considérées comme propres à leur auteur »

REMERCIEMENTS

Qu'il me soit permis de remercier Madame Frédérique CHOPIN pour ses conseils et son investissement tant dans le cadre de ce mémoire que dans les enseignements qu'elle a dispensés durant cette année.

LISTE DES ABRÉVIATIONS

AJ Pénal	Actualité juridique pénal
Ass. plén.	Assemblée plénière de la Cour de cassation
[B]	Arrêt publié au bulletin
Cass. crim	Chambre criminelle de la Cour de cassation
CEDH	Cour européenne des droits de l'homme
Cons. Const.	Conseil constitutionnel
Conv. EDH	Convention européenne des droits de l'homme
C. pr. civ	Code de procédure civile
C. pr. pén.	Code de procédure pénale
C. civ.	Code civil
C. pén.	Code pénal
C. mon. fin.	Code monétaire et financier
Déc.	Décision
Dr. banc	Revue Droit bancaire, LexisNexis
Dr. pénal	Revue Droit pénal, LexisNexis
Gaz. Pal	Gazette du palais
In	Dans, extrait de
IP/IT	Dalloz IP/IT - droit de la propriété intellectuelle et du numérique
JCP G	La semaine juridique, édition générale
L	Loi
PSAN	Prestataire de service sur actifs numérique
PUF	Presse universitaire de France
n°	Numéro
QPC	Question prioritaire de constitutionnalité
RSC	Revue de science criminelle et de droit pénal comparé
UE	Union européenne

SOMMAIRE

INTRODUCTION

Sans anachronie, il est permis d'assimiler la blockchain à une activité productive de type traditionnel et souscrire ainsi à la conception smithienne de la division du travail. En effet :

« Dans chaque art, la division du travail, aussi loin qu'elle peut y être portée, donne lieu à un accroissement proportionnel dans la puissance productive du travail[1] *».*

Adam Smith, *Recherches sur la nature et les causes de la richesse des nations*

La coopération entre êtres humains est au fondement même du progrès. Elle permet la mise en commun des capacités et la répartition des fardeaux. Sa négation est source de conflits, sa magnificence est force de création. Il n'est pas de meilleur exemple que celui offert par Adam SMITH dans ses *Recherches sur la Nature et les Causes de la Richesse des Nations* à propos de la division du travail. L'auteur écossais prenait ainsi l'exemple de la fabrication d'une épingle : "*(...) un ouvrier lit le fil à la bobille, un autre le dresse, un troisième coupe la dressée, un quatrième empointe, un cinquième est employé à émoudre le bout qui doit recevoir la tête. Cette tête est elle-même l'objet de deux ou trois opérations séparées : la frapper est une besogne particulière ; blanchir les épingles en est une autre; c'est même un métier distinct et séparé que de piquer les papiers et d'y bouter les épingles ; enfin l'important travail de faire une épingle est divisé en dix-huit opérations distinctes ou environ, lesquelles, dans certaines fabriques, sont remplies par autant de mains différentes (...)".*

La blockchain répond à cette logique, quand bien même, à la différence de la production d'une épingle, la division du travail a lieu entre plusieurs machines exécutant une opération unique de résolution de problèmes informatiques. Elle fait sourdre en creux le caractère par nature organisé de son déploiement, ce qui se ressent notamment sur les enjeux qu'elle fait naître.

[1] A. SMITH, *Recherches sur la nature et les causes de la richesse des nations,* 1776, W. Strahan and t. Cadell, Londres.

1. - Notion de blockchain. La blockchain ou "chaine de blocs" en français est une " *base de données ou registre regroupant la liste de tous les échanges effectués entre ses utilisateurs depuis sa création*[2]*".* Elle peut à cet égard être comparée à un registre dans lequel seraient enregistrés tous les échanges ayant eu lieu entre plusieurs individus et inscrits dans cette blockchain. Cependant, au lieu d'être tenue par une seule et même entité à l'instar d'un registre traditionnel, la blockchain est décentralisée. Cela signifie que, sous certaines conditions, toute personne peut y apporter des modifications en y ajoutant un bloc, lequel contient lui-même des informations. Plus précisément, Les blockchains sont des *« technologies de stockage et de transmission d'informations, permettant la constitution de registres répliqués et distribués, sans organe central de contrôle, sécurisées grâce à la cryptographie, et structurées par des blocs liés les uns aux autres, à intervalles de temps réguliers*[3] *»*. Cette définition permet de présenter les caractéristiques de la blockchain.

2. - Des blockchains ? Tout d'abord, il est préférable de parler de blockchains au pluriel. En effet, les formes que peut prendre cette technologie sont variées et répondent toutes à un fonctionnement différencié. Elle peut ainsi être publique et accessible à tous. Il s'agit de la conception la plus commune. Les utilisateurs peuvent y inscrire des informations et s'en servir librement à diverses finalités - transaction, stockage de données, création de jetons, mise en place de smart contracts etc. Elle répond au concept d'open source[4], qui est un logiciel dont le code source est ouvert et qui peut être ainsi modifié par tous. Dans cette configuration, la blockchain est un registre distribué et décentralisé.

Mais plus rarement, la blockchain peut être privée et dès lors reposer sur un système centralisé et géré par une entité désignée et identifiée qui peut en contrôler l'accès au moyen, notamment, d'un identifiant. Cette catégorie s'éloigne de la première en ce qu'elle n'est plus une technologie en open source mais une technologie en source fermée. Elle peut par exemple être utilisée par une entreprise privée pour la conservation et l'échange de données internes.

3.- Cryptographie. Le fonctionnement et l'intégrité de ces registres reposent notamment sur le recours à des moyens de cryptologie se définissant par l'ensemble des procédés permettant de rendre une information intelligible en l'absence de la clef de déchiffrement idoine. La blockchain

[2]M. QUEMENER, *Le Droit face à la disruption numérique*, Gualino, 2018, p.42.
[3] V. FAURE-MUNTIAN, C. DE GANAY, R. LE GLEUT, rapport au de l'Office parlementaire des choix techniques et scientifiques sur *Les enjeux des blockchains*, (chaîne de bloc), 20 juin 2018.
[4] M. QUEMENER, op., cit., p. 43.

utilise la cryptographie asymétrique. Ce système repose sur deux clés de cryptographie différentes : la clef publique, pour chiffrer, l'autre, la clef privée, pour déchiffrer. L'utilisateur qui souhaite recevoir des messages engendre un tel couple de clefs. Quiconque souhaite lui envoyer un message confidentiel utilise la clef publique pour chiffrer celui-ci. Le message chiffré obtenu ne peut être déchiffré qu'en connaissant la clef privée[5]. Dans le cas d'une transaction par le biais de la blockchain, l'information est tout d'abord cryptée par une clef publique sous la forme d'un *hash* de transaction, *id est*, une suite de caractères correspondant à l'information cryptée. Par exemple, l'expression *principe non bis in idem* devient, une fois cryptée : *333000C20E40ED6A590CC0F29AC2BF78*

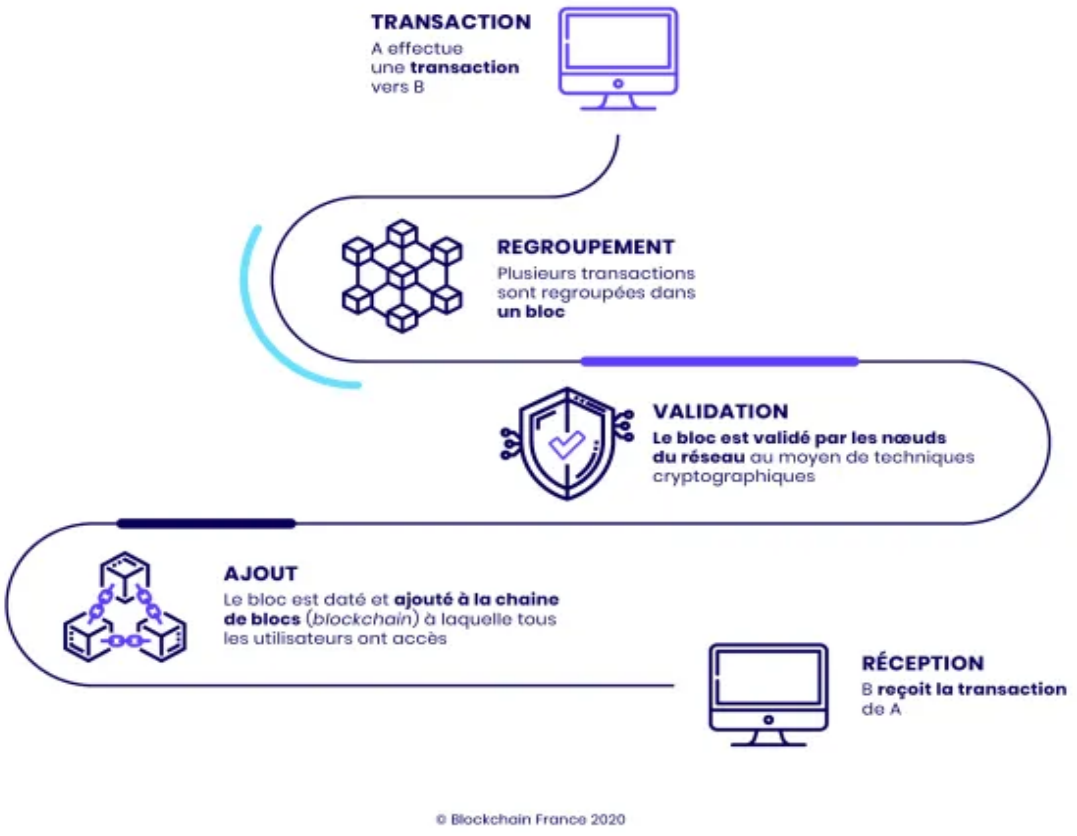
Une fois l'information cryptée, elle peut être envoyée vers un bloc de transaction. Ce dernier sera par la suite validé puis, le cas échéant intégré à la blockchain. In fine, la personne qui recevra le hash de transaction pourra décrypter l'information au moyen de sa clef privée. Cette modalité d'échange est donc une garantie forte en termes de sécurisation des transactions, sous réserve pour chacun de ne pas perdre la clef privée sans laquelle l'information est définitivement inaccessible. Ainsi, un Américain, Stefan THOMAS, ayant stocké en 2011 près de sept milles bitcoins sur un portefeuille duquel il a perdu la clef privée[6]. Son préjudice s'élève aujourd'hui à environ cent dix millions de dollars.

4. - Blocs de transaction. Comme énoncé précédemment, la technologie blockchain est un registre distribué. Ce faisant, elle peut être incrémentée par tous utilisateurs disposant a minima d'un ordinateur et d'une clef publique. La notion de bloc sur laquelle elle repose renvoie au processus d'enregistrement des transactions dans la blockchain. Un bloc représente une somme de transactions réalisées par les utilisateurs. Ce bloc va par la suite être validé par les "nœuds" de réseaux sous l'action de mineurs - qualifiés de la sorte en raison de leur puissance de travail à l'instar des travailleurs des mines. Pour valider un bloc de transaction, plusieurs moyens sont possibles selon la nature de la blockchain. Le plus connu est celui propre au bitcoin et consiste en une preuve de travail ou proof of work. Les mineurs devront effectuer des calculs complexes et particulièrement énergivores pour confirmer la transaction en contrepartie d'une rémunération, en l'espèce en bitcoins. Une fois validé, le bloc est horodaté puis intégré dans la blockchain. Il sera

[5] https://fr.wikipedia.org/wiki/Cryptographie_asym%C3%A9trique
[6] https://journalducoin.com/bitcoin/multimillionnaires-bitcoins-perdu-acces/

désormais accessible à tous et ne pourra plus être modifié[7]. Cette validation sera également la condition de réalisation de la transaction s'il s'agit de la finalité poursuivie ab initio.

Ce schéma offert par le site *Blockchain France* permet d'illustrer le fonctionnement simplifié d'une blockchain.



[7] https://blockchainfrance.net/decouvrir-la-blockchain/c-est-quoi-la-blockchain/

5. - Caractéristiques de la blockchain. Le fonctionnement de cette technologie lui confère des caractéristiques particulières. Elles diffèrent selon que la blockchain est dite publique ou privée. S'agissant de la forme la plus répandue, seules les spécificités de la blockchain ouverte seront présentées. En ce qui concerne la blockchain privée, elles varient grandement selon les règles fixées par l'entité qui en assure la gestion.

5.1.-Décentralisation. Tout d'abord, l'absence d'entité centrale permet à chaque individu d'introduire des données dans un bloc et de contribuer à sa validation. En parallèle, il n'existe pas de contrôle a priori de l'intégrité de ces informations ni de leur contenu. Ainsi, *"la blockchain n'appartient à personne et elle appartient à tous, selon des règles fixes et transparentes de fonctionnement – le protocole informatique – connues de tous*[8]*"***.** Par conséquent, elles peuvent être de toute nature et par là même illicite[9]. Cette absence d'autorité de contrôle n'est pas compensée par l'existence d'une validation a posteriori de la transaction dès lors que son contenu est présenté sous forme d'un hash que seul le propriétaire de la clef privée y afférente pourra déchiffrer.

5.2 - Transparence. En ce que la blockchain publique est accessible à tous, elle est par nature transparente. Toutefois, cette notion ne saurait s'entendre comme permettant à toute personne de connaître exactement et en temps réel le contenu de la blockchain. Seules les transactions ayant été validées et intégrées dans cette dernière sont visibles. Plus précisément, les utilisateurs agissent par l'intermédiaire de clefs publiques et ne révèlent pas leur identité. Partant, ils sont connus sous leur adresse publique plutôt que sous leur nom. Il est donc impossible de savoir qui se cache derrière une adresse publique donnée, en tout cas lorsqu'aucune information n'a été divulguée quant à l'identité de l'utilisateur au moment de la création de l'adresse. Les utilisateurs peuvent d'ailleurs avoir plusieurs adresses. Mais en dehors de cet anonymat, ou plutôt de ce pseudonymat, l'ensemble des transactions peut être suivi par les tiers. Pour ce faire, il n'y a qu'à se rendre sur l'un des sites de suivi de blockchain tel que le site Blockchain.com[10].

5.2 - Intégrité et immutabilité. Parce que chaque transaction doit être validée au sein de chaque bloc avant d'être intégrée à la blockchain, elle ne peut être modifiée de manière arbitraire. À cet

[8] *Sur les chaînes de blocs (blockchains)*, Rapport d'information n°1501 déposé par la Mission d'information commune sur les chaînes de blocs et présenté par Mme Laure De La RAUDIÈRE et M. Jean-Michel MIS, 12 juin 2018.
[9] Cette problématique sera envisagée plus en avant dans le cadre de la partie consacrée à la criminalité relative à la blockchain.
[10] https://www.blockchain.com/explorer

égard, deux couches d'immutabilité se superposent[11]. Le registre est tout d'abord formé par une chaîne de blocs qui s'ajoutent les uns aux autres. Dès lors, le bloc suivant contient les informations du bloc précédent si bien que la modification du premier emporte celle du deuxième puis du troisième etc. Dès lors, *"si un bloc de données est modifié, le hachage de ce bloc change et ne correspondra pas au hachage stocké dans le bloc suivant. Si cela se produit, tous les blocs suivants seront automatiquement écartés[12]"*. Pour valablement modifier ou supprimer l'information, il faudrait donc remonter à l'origine de la première transaction et agir sur cette dernière et ce, pour chaque copie conservée par chacun des utilisateurs de la blockchain[13]. De plus, le processus de validation des blocs est lui-même source d'immutabilité car, pour qu'une opération soit intégrée dans la blockchain, elle doit passer entre les fourches caudines d'au moins 51 % des mineurs[14]. C'est pourquoi la blockchain est souvent présentée comme infalsifiable : la modifier nécessiterait une puissance de calcul colossale qui, pour une blockchain comme le Bitcoin, serait à l'heure actuelle inenvisageable[15], sauf à utiliser la puissance d'un ordinateur quantique[16].

6. - Applications de la blockchain. La chaîne de blocs n'est donc pas une réalité autonome. Il s'agit en réalité d'une technique d'identification et d'enregistrement des informations, renforcée par son caractère décentralisé. Ainsi, elle peut être mise au service de différentes institutions. Seront présentées, par souci d'exhaustivité, les principales applications de la blockchain qu'il s'agisse des crypto-monnaies, des jetons non-fongibles, des smarts contracts et du métavers. Leur point de convergence est qu'elles sont toutes fondées sur le principe de neutralité. A priori dépourvus de toutes finalités criminelles, ces outils peuvent être dévoyés et utilisés en tant que cible ou vecteur d'une infraction. C'est la raison pour laquelle il apparaît nécessaire d'en connaître le fonctionnement simplifié pour appréhender les défis qu'ils font émerger.

---

[11] F. G'SELL F. MARTIN-BARITEAU, L'impact des blockchains sur les droits de l'homme, la démocratie et l'État de droit, Rapport rédigé pour le Conseil de l'Europe, mars 2022

[12] ibid

[13] H, JEAN-BENOIT, La preuve par la blockchain. In Les blockchains et les smart contracts à l'épreuve du droit, p. 185-208, Collection du CRIDS; No. 49, 2020

[14] Pour qu'une transaction soit validée, plus de la moitié des nœuds du réseau blockchain doivent avoir réussi l'opération de calcul prévue à titre de preuve de travail. Cette exigence quantitative est l'une des garanties majeures de l'intégrité du système.

[15] Il est à noter toutefois qu'une telle prise de pouvoir par un groupe de cyberdélinquant ou un pays ennemi serait possible à l'encontre de blockchain de plus faible envergure. Il s'agit alors d'une attaque 51 % à laquelle il sera fait allusion plus en avant.

[16] M.WEBBER, V. ELFVING, S. WEIDT et al., "The impact of hardware specifications on reaching quantum advantage in the fault tolerant régime", *AVS Quantum* Sci. **4**, 013801 (2022). Dans cette étude, des chercheurs de l'Université de Sussex en Angleterre estiment qu'un ordinateur disposant de 13 millions de qubits pourrait pirater une blockchain en moins de 24 heures et ainsi en prendre le contrôle.

6.1 - Les crypto-monnaies. Terme dont l'étymologie provient du grec *kruptós* qui signifie caché et du latin *moneta*, les crypto-monnaies se conçoivent au pluriel. Il y aurait entre 1300[17] et 16000[18] monnaies virtuelles différentes actuellement en circulation. Toutefois, d'aucuns estiment que près de 1000 nouvelles crypto-monnaies seraient créées chaque mois pour une capitalisation totale de 2000 milliards de dollars selon la plateforme de trading Crypto Parrot[19]. Cette incertitude entourant ces actifs est liée à l'idéologie qui les sous-tend. Si elles sont apparues dans les années 1990 sans rencontrer de succès avec notamment le Digicash, ce n'est qu'en 2009 qu'apparaît le Bitcoin, crypto-monnaie la plus répandue et la plus connue. Son créateur - réel ou mythifié - serait Satoshi Nakamoto qui décrivit les fonctionnalités de cette blockchain dans un livre blanc publié le 31 octobre 2008 et intitulé "*Bitcoin – A Peer to Peer Electronic Cash System*[20]*"*. La volonté de ces créateurs était alors de fonder un système de transactions décentralisé et dépourvu d'institution. L'idéologie sous-jacente est alors proche des anarchistes appelés également *cypherpunk*, qui souhaitaient garantir leur vie privée par le recours à la cryptographie. Aujourd'hui, bien plus qu'un simple outil de confidentialité, les monnaies virtuelles sont devenues des instruments hautement spéculatifs, dont la volatilité importante leur offre un attrait croissant.

Les institutions nationales ne reconnaissent pas à ces technologies le caractère de monnaie[21] fussent-elles virtuelles. En effet, le législateur qualifie les crypto-monnaies de "t*oute représentation numérique d'une valeur qui n'est pas émise ou garantie par une banque centrale ou par une autorité publique, qui n'est pas nécessairement attachée à une monnaie ayant cours légal et qui ne possède pas le statut juridique d'une monnaie, mais qui est acceptée par des personnes physiques ou morales comme un moyen d'échange et qui peut être transférée, stockée ou échangée électroniquement* [22]". Il s'agit donc de biens meubles incorporels *sui generis* dont la valeur repose sur la confiance des opérateurs. La jurisprudence reconnaît expressément cette classification[23]. Cependant, aux fins de cohérence et de simplification de la rédaction, les termes de

[17] J. FONTANEL. Le crime international organisé et les cryptomonnaies. " Les Géopolitiques " de Brest, Université de Bretagne Occidentale (UBO); IMT Atlantique; ENSTA Bretagne; École navale, Feb 2022, Brest, France.
[18] G. DE WARREN, Enjeux et risques des crypto-actifs, Rapport de la Direction générale du Trésor, juin 2022
[19] https://cryptoparrot.com/
[20] https://www.cryptovantage.com/fr/guides/une-breve-histoire-de-la-cryptomonnaie/
[21] Rapport de la Banque de France, "Les dangers liés au développement des monnaies virtuelles : l'exemple du bitcoin", 5 décembre 2013 précisant que *"le bitcoin ne peut pas être qualifié de monnaie ayant cours légal dans la mesure où il est possible de le refuser en paiement sans contrevenir aux dispositions de l'article R642-3 du Code pénal, qui sanctionne le refus d'accepter les billets et les pièces libellés en euros ayant cours légal. Sa mise en circulation ne violerait donc pas le monopole d'émission de la monnaie ayant cours légal des banques centrales".*
[22] C. mon.fin., art. L.54-10-1.
[23] CA Paris, 26 sept. 2013, n° 12/00161, Macaraja c/Crédit industriel et commercial : *"le bitcoin n'est pas une monnaie électronique mais un bien immatériel non soumis à la législation sur les monnaies électroniques"*

crypto-monnaies, monnaies virtuelles ou encore d'actifs numériques seront indistinctement usités pour désigner cette même réalité.

6.2 - Les jetons non fongibles. Aussi dénommés *non fungible token* en anglais. Il s'agit de jetons émis et authentifiés par une blockchain et qui ont la particularité d'être uniques. En effet, à la différence des crypto-monnaies, les jetons ne sont pas interchangeables entre eux et peuvent ainsi être précisément identifiés. Cette caractéristique leur octroie une dimension originale en ce qu'ils peuvent représenter n'importe quel caractère et faire l'objet de ventes aux enchères et atteindre des sommes importantes[24]. Ces actifs uniques sont susceptibles d'être utilisés dans plusieurs domaines que ce soit celui des jeux vidéo, de l'art, dans les métavers ou encore à titre utilitaire pour accéder à un bien ou un service[25].

6.3. - Les smarts contracts. Si l'autonomie de la volonté est érigée en principe cardinal du droit civil des contrats[26], il en va également ainsi en matière de blockchain où la liberté est la règle. Les smarts contracts ou " contrats intelligents", sont des protocoles informatiques qui prévoient l'exécution automatique de certaines tâches ou opérations lorsque certaines conditions sont réunies[27]. Ainsi, il ressort de cette définition que les smarts contracts sont en réalité des protocoles enregistrés dans une blockchain afin d'effectuer des tâches préalablement inscrites dans leur code source. Ils permettent dès lors d'automatiser un processus. Leur application est infinie et leur association à la technologie de la chaîne de blocs leur assure une sécurité renforcée. Cependant, là encore, la neutralité ontologique des contrats intelligents est susceptible d'être instrumentalisée à des fins criminelles dans la mesure où ces derniers peuvent exécuter des actions répétées pouvant constituer des infractions d'habitude comme le harcèlement moral[28], les menaces réitérées[29] ou encore les appels téléphoniques malveillants[30].

---

[24] "*Le 11 mars 2021, l'artiste américain Beeple a vendu aux enchères une œuvre numérique pour un montant de 69,3 millions de dollars, faisant de lui le troisième artiste le plus cher au monde derrière David Hockney et Jeff Koons",*
J. PROST et A. JEAN-BAPTISTE, " Les Non-fungible tokens saisis par le droit" , *Dalloz IP/IT,* 5, mai 2022, p. 260-267

[25] Ibid

[26] C. Civ., art. 1172 al.1 : *"Les contrats sont par principe consensuels".*

[27] F. G'SELL F. MARTIN-BARITEAU, préc.

[28] C. pén., art. 222-33 : Le fait de harceler autrui par des propos ou comportements répétés ayant pour objet ou pour effet une dégradation des conditions de travail susceptible de porter atteinte à ses droits et à sa dignité, d'altérer sa santé physique ou mentale ou de compromettre son avenir professionnel, est puni de deux ans d'emprisonnement et de 30 000 € d'amende.

[29] C. pén., art. 222-17 al. 1 : "*La menace de commettre un crime ou un délit contre les personnes dont la tentative est punissable est punie de six mois d'emprisonnement et de 7 500 euros d'amende lorsqu'elle est, soit réitérée, soit matérialisée par un écrit, une image ou tout autre objet".*

[30] C. pén., art. 222-16 : Les appels téléphoniques malveillants réitérés, les envois réitérés de messages malveillants émis par la voie des communications électroniques ou les agressions sonores en vue de troubler la tranquillité d'autrui sont punis d'un an d'emprisonnement et de 15 000 euros d'amende.

6.3 - Métavers ou métavers ? Issu de la contraction des termes *méta* qui signifie au-delà et *univers* qui signifie monde, le Métavers est un *"service en ligne donnant accès à des simulations d'espaces 3D temps réel, partagées et persistantes, dans lesquelles on peut vivre ensemble des expériences immersives*[31]". Il s'agit d'un univers accessible via un dispositif technique et mettant en relation différents individus évoluant au sein d'une réalité virtuelle ou augmentée. Le concept du Métavers, qui se distingue de ses différentes déclinaisons en métavers, est apparu sous la plume de l'écrivain américain Neal Stephenson dans *Snow Crash* en 1992. Il a progressivement été développé dans le domaine des jeux vidéo et offre aujourd'hui un horizon de possibles substantiel, si bien qu'une véritable industrie des métavers se fait jour. Si le Métavers n'est pas par essence fondé sur la blockchain, celle-ci lui est fréquemment associée en ce qu'elle permet de lui assurer sa permanence et qu'elle est également le vecteur des crypto-monnaies et des jetons, actifs utilisés dans cet univers.

Les enjeux que représente le Métavers sont majeurs. En effet, son potentiel immersif et sa persistance le rendent propice à toutes formes de dérives illicites. En sus, l'anonymat que permet le recours à des avatars et des pseudonymes est une source de difficulté pour les autorités de poursuites. Enfin, le Métavers pose des questions en termes d'application de la loi pénale qui seront abordées dans le cadre de ces développements.

7. - Notion de criminalité. Selon le Larousse, la criminalité est *"l'ensemble des actes criminels et délictueux commis dans un groupe donné à une époque donnée*[32]*"*. Le terme de criminalité employé ici rejoint cette acception large qui entend inclure l'activité de tous ceux qui enfreignent la loi pénale. Plus précisément selon MERLE et VITU, "*entre le crime et la criminalité, il y a une simple nuance quantitative. Le crime est un acte isolé, individuel ou collectif. La criminalité est un état social composé par la globalisation des crimes qui perturbent la société*[33]*"*.

Partant, ce phénomène est par nature évolutif et s'adapte aux innovations de la société. La technologie a représenté pour la criminalité un levier d'amélioration de son efficacité et de développement de son impunité. A cet égard, le terme de cybercriminalité a émergé pour appréhender un phénomène en constante affirmation.

[31] A.BASDEVANT C. FRANCOIS R. RONFARD, Mission exploratoire sur les métavers, octobre 2022
[32] Dictionnaire Larousse (éd. 2000)
[33] R. MERLE, A. VITU, *Traité de droit criminel,* Cujas 7e édition, 2000.

8. - La cybercriminalité. Il s'agit de *"toute infraction pénale tentée ou consommée au moyen ou à l'encontre d'un système d'information et communication, principalement Internet[34]"* . Cette forme particulière de la criminalité repose sur l'emprise des technologies de l'information sur les différents champs de la vie humaine. Elle en exploite les failles ou les détournent de leur but pour commettre des infractions. Le terme de criminalité renvoie à l'ampleur de ces actes qui toucheraient chaque année 978 millions de personnes dans le monde[35]. Aussi, pour lutter contre ce fléau grandissant, le législateur et l'autorité judiciaire tentent d'adapter le droit en général et le droit pénal en particulier afin qu'il soient aptes à encadrer et sanctionner ces actes. Le premier par la multiplication des textes de circonstance - dont la liste même énumérative ne serait pas pertinente pour le sujet traité - la seconde par un travail d'interprétation et de qualification constructif.

8.1. - La force créatrice du juge pénal. Face au décalage entre la célérité de l'évolution des nouvelles formes de criminalité et la lenteur du système juridique à saisir, analyser et répondre, le juge pénal est amené à sortir du cadre strict du principe de légalité criminelle. Nombreuses en sont les illustrations. Ainsi, dès 1912, la Cour de cassation a pu considérer que la qualification de vol pouvait être retenue à l'encontre de celui qui captait indûment l'électricité d'autrui[36] ou encore que le fait d'envoyer des messages malveillants de manière réitérée pouvait caractériser l'infraction d'appels téléphoniques malveillants[37]. Il est donc dans la praxis des juges répressifs et plus particulièrement de la Chambre criminelle de la Cour de cassation d'étendre l'assiette d'un texte ou d'en assouplir les conditions d'application. En effet, *"les incriminations de droit pénal classique connaissent des distorsions finalistes justifiées par les besoins de la répression"*[38].

9. - Technologies 3.0. Le dernier état de l'art numérique se profile sous les auspices du Web 3.0. Entendu comme l'ensemble "*des applications et plateformes décentralisées développées et opérant sur des blockchains publiques et parfois soutenues par des tokens non fongibles*[39]*",* il s'agit donc de la nouvelle forme d'interaction sur Internet reposant sur la décentralisation permise par la technologie blockchain. Dès lors, elle assure une désintermédiation généralisée à l'ensemble de la communauté d'Internet des échanges et des transactions. Elle se caractérise par la rapidité et la

[34] F. CHOPIN, " Cybercriminalité", *Répertoire de droit pénal et de procédure pénale*, Dalloz 2020, 497 pages
[35] Ministère de l'Intérieur et des Outre-Mer, "Cybercriminalité : l'action du ministère", Actualités 2019.
[36] Crim. 3 août 1912 : DP 1913. 1. 439 ; S.1913. 337, note ROUX.
[37] Crim. 30 sept. 2009, pourvoi n°09 - 80. 379.
[38] C. GHICA-LEMARCHAND, *L'interprétation de la loi pénale par le juge,* Colloque sur l'office du juge au Sénat, 29 et 30 septembre 2006.
[39] Cryptoast.com, "Qu'est-ce que le Web3, cette version décentralisée d'Internet ? ", 22 novembre 2022 (consulté le 10 décembre 2022).

confidentialité. Aussi, les technologies 3.0 qui empruntent cette voie représentent un défi considérable pour les pouvoirs publics. En conséquence, législateur et autorité judiciaire sont et seront soumis à une tension forte entre impératif de sécurité et garantie de liberté. Cette double volonté a priori antinomique, voire oxymorique, n'est en réalité qu'une constante du droit pénal aujourd'hui confronté à des dispositifs qui le dépassent.

10. - Champ d'étude. Les enjeux que sous-tend la blockchain sont nombreux et leur étude exhaustive dépasserait le cadre d'un simple mémoire de recherche. Il sera en effet question en l'espèce de la confrontation, mais aussi de la relation entre le droit répressif et la technologie blockchain. S'agissant de la notion de droit répressif, elle veut englober à la fois le droit pénal de fond - incriminations, responsabilité pénale, sanctions pénales - et le droit pénal de forme - investigations, jugement, exécution des peines. Mais elle inclut également, dans une acception extensive, les dispositifs préventifs permettant de limiter ou de prévenir les faits de cybercriminalité. En effet, comme pour toute forme de criminalité, une réponse globale et effective doit se déployer tant en amont qu'en aval du passage à l'acte. La prévention de la criminalité est aussi importante que sa répression, sinon plus. Dès lors, la notion de droit répressif sera holistique et couvrira l'ensemble des dispositifs de lutte contre cybercriminalité blockchain.

S'agissant de la notion générique de blockchain - dont il a été précisé qu'il s'agit en réalité d'une technique plus que d'une technologie - elle sera nécessairement circonscrite à ses émanations les plus disruptives et les plus répandues dans le champ criminel. Pour parler de cette technologie, les termes de blockchain ou de chaîne de blocs seront indifféremment employés.

11. - Problématique. Traiter d'un sujet général comme la criminalité en relation avec une notion complexe et spécifique comme la blockchain amène à s'interroger sur la pertinence d'un tel choix. En effet, il pourrait être soutenu que la technologie de la chaîne de blocs, bien qu'étant révolutionnaire in abstracto, ne bouleverse pas l'appréhension de la criminalité de manière telle qu'elle en justifierait une remise en cause. Il serait possible d'appliquer les critères classiques de la cybercriminalité en les adaptant à la marge pour qu'ils recouvrent ces nouvelles modalités de commission d'une infraction.

Toutefois, ce serait négliger que la blockchain est bien plus qu'une technique innovante. Il s'agit d'une façon de penser, une vision du monde en rupture avec les codes établis. Les cybercriminels qui y adhèrent sont en négation avec l'État et son système de valeur. Le phénomène criminologique

de la blockchain doit donc être présenté en ce qu'il incarne à la fois une forme nouvelle de criminalité mais également une idéologie. Cette idéologie résulte de l'histoire même de la blockchain.

Promue par le mouvement des *cypherpunk* - de *cypher* signifiant cryptologie et *punk* signifiant rebelle, la blockchain est en effet l'une des dernières étapes de l'affirmation croissante de cette contre-culture de l'informatique. À cet égard, il importe de citer l'exemple de la Déclaration d'indépendance du cyberespace prononcée en 1996 par l'Américain J. PERRY BARLOW[40], aux termes de laquelle il refuse l'appropriation d'Internet par un Gouvernement extérieur et notamment celui des États-Unis. Cette prise de position, certes symbolique, est cependant révélatrice de la pensée de ces militants qui dénient toute légitimité aux formes institutionnalisées de gouvernance. La prétention de ces protagonistes était et demeure in fine de remplacer la confiance dans une institution centralisée par la confiance dans les divers processus cryptologiques et informatiques. *Code is law*[41] devient ainsi le mantra de ces acteurs et affirme la prévalence du code sur la loi.

Cette montée en puissance de la blockchain aboutit à l'émergence de nouvelles inquiétudes pour les autorités étatiques ou les simples particuliers et ce en raison de ses usages présents et à venir ainsi que de son caractère encore méconnu.

11.1. - Aussi, face aux possibilités offertes par la technologie blockchain et au regard de l'état actuel des dispositifs répressifs, il sera nécessaire de s'interroger sur leur efficacité. Cela conduit à s'interroger de la façon suivante : ***Comment le droit répressif peut-il lutter contre l'usage de la blockchain à des fins criminelles ?***

12. - Dichotomie de la réflexion. Pour tenter d'apporter une réponse à cette problématique, les développements qui suivent seront scindés en deux idées-forces. Tout d'abord, il s'agira de tenter d'identifier les phénomènes criminels permis ou facilités par la technologie blockchain et ses dérivés. Cette première étape fondamentale permettra en effet de connaître l'état et l'acuité de la menace qui pèse sur la société. Une fois assimilés, ces risques seront confrontés aux forces et faiblesses dont disposent les institutions de lutte et de prévention de la criminalité, afin de souligner les limites de ces dispositifs et de proposer des axes d'améliorations.

[40] H. D'AGRAIN, « Géopolitique de l'espace numérique. Quelles stratégies de sécurité ? », Futuribles, 2022/6 (N° 451), p. 21-37.
[41] L.LESSIG, Code is Law – On Liberty in Cyberspace, Harvard Magazine, janvier 2000.

12.1 - Deux parties seront classiquement distinguées afin d'élaborer cette analyse. Chacune d'entre elles sera alimentée par une réflexion plus profonde sur les enjeux sociétaux et l'équilibre nécessaire entre encadrement et innovation, répression et tolérance.

Dans la première partie, les phénomènes de criminalité mis en lumière procéderont d'un choix arbitraire. Cet arbitraire ne devra pas être entendu dans son acception négative de *"ce qui dépend de la volonté, du bon plaisir de quelqu'un et intervient en violation de la loi ou de la justice*[42]*",* mais de son acception originelle de ce qui est arbitré, pesé par le juge afin de choisir la solution la plus conforme au sens ancien de *l'arbitrium judicis*[43]. Or, l'ampleur des infractions couvertes par les usages potentiels de la blockchain contraindra cette étude à un choix fondé sur leur prévalence et leur probabilité de nuisance. Malgré cette éviction méthodologique, les développements suivants permettront de cerner un phénomène grandissant par son ampleur et ses effets. Sera donc défendue dans un premier temps l'idée que la blockchain peut être une technologie innovante vectrice d'une criminalité 3.0 (**PREMIÈRE PARTIE**).

Dans un second temps, l'approche consistera en une présentation des mesures répressives destinées à réagir à cette nouvelle forme de criminalité. Ces mesures reposant soit sur des dispositifs traditionnels mais actualisés pour s'adapter à la blockchain, soit sur de nouveaux instruments innovants. En effet, il est à noter que la blockchain n'est qu'une illustration parmi d'autres des ruptures technologiques ayant contraint les acteurs de la lutte contre la criminalité à s'adapter. L'intérêt de cette étude réside en ce que cette technologie est l'une des plus récentes dans l'histoire des innovations et qu'elle constitue de ce fait un défi majeur. Pour mettre en œuvre cette réponse pénale, la complexité sera de définir un cadre d'action cohérent et complet passant de la prévention à la répression, ce qui, en l'état actuel n'est pas encore acquis. C'est donc la nécessaire évolution du droit pénal qui sera questionnée. (**SECONDE PARTIE**).

[42] Dictionnaire Larousse.
[43] C. GAU-CABÉE, *Arbitrium judicis. Jalons pour une histoire du principe de la légalité des peines*, L.G.D.J, 2007.

Première partie

La blockchain, technologie innovante vectrice d'une criminalité 3.0

13.- Par ses nombreuses applications, la blockchain constitue une source potentielle de criminalité. Les caractéristiques de décentralisation et de discrétion offertes à ses utilisateurs contribuent à en rendre l'appréhension difficile par les autorités publiques et alimentent ainsi leur défiance. La blockchain est en effet une arme pour les cybercriminels qui sont par principe susceptibles d'en maîtriser les différents usages. Ces derniers pourraient s'en servir à la fois pour commettre l'infraction mais également pour la préparer, voire en assurer l'impunité.

Dans la première hypothèse, la blockchain intervient au cœur même de l'infraction, elle en est la condition sine qua non. Si sa démocratisation la rend plus accessible, les formes de criminalité qu'elle ouvre sont a priori celles couvertes par les champs de la criminalité organisée et par essence internationale. En effet, *"plus un bien ou service est interdit, et plus il est rare, risqué et donc cher. Le domaine de l'économie digitale intéresse le crime organisé car des actions illégales mais économiquement très fructueuses peuvent être engagées[44]"*. Ainsi, blockchain et cybercriminalité organisée vont de pair dans un monde virtuel soumis à la loi du plus fort et donc du mieux organisé. Ces organisations profitent également de leur implantation dans le cyberespace qui peut se définir comme *"un ensemble de données numérisées constituant un univers d'information et un milieu de communication, lié à l'interconnexion mondiale des ordinateurs[45]"*. Ce territoire, théorisé en 1984 par William GIBSON[46], correspond à *"un espace virtuel dont l'accès est possible grâce à une connexion et qui permet d'exercer certaines activités[47]"*. Il s'agit pour certains d'un territoire à l'instar de la terre, la mer et l'air et qui permet à ceux qui en ont la maîtrise de naviguer en toute discrétion, voire, en toute impunité. Il jouera donc un rôle fondamental dans la commission des infractions relatives à la blockchain et sera abordé en conséquence au fur et à mesure de cette recherche. Dès lors, il conviendra de se demander comment ces organisations réussissent à placer la blockchain au coeur de l'infraction **(TITRE I)**

---

[44] J. FONTANEL. Le crime international organisé et les cryptomonnaies. " Les Géopolitiques " de Brest, Université de Bretagne Occidentale (UBO); IMT Atlantique; ENSTA Bretagne; École navale, Feb 2022, Brest, France.

[45]Dictionnaire Le Robert de poche 2019.

[46] GIBSON W., Neuromancien, 1984, in N. OUCHENE*, L'applicabilité de la loi pénale à l'endroit de la cybercriminalité dissimulée.,* Droit, Université Paris 2 Panthéon-Assas, 2018.

[47] ibid.

Dans une seconde hypothèse, la criminalité induite par la chaîne de blocs se conçoit en périphérie de l'infraction principale. Il s'agit alors de saisir des comportements antérieurs ou postérieurs qui recèlent cependant une dangerosité intrinsèque. Ils imposent alors de prendre en compte les risques engendrés par cette méthode sans pour autant en entraver trop strictement l'expansion. Dans un marché en pleine dilatation[48] et ouvrant à des solutions techniques formidables, il serait contre-productif de tuer dans l'œuf toute utilisation de la blockchain. Aussi, face à l'impératif sécuritaire vu au prisme d'enjeux économique et sociétaux majeurs, la blockchain doit être encadrée pour saisir les frontières de l'infraction **(TITRE II)**

Titre I. La blockchain au cœur de l'infraction

14.- Dire que la blockchain est au cœur de l'infraction ne suffit pas. Il faut souligner au préalable une dichotomie souvent usitée en matière d'infractions commises au moyen des technologies de l'information. En effet, les différents instruments internationaux ou textes relatifs à la cybercriminalité dressent une *summa divisio* au sein de cette forme de criminalité. Ainsi, ils distinguent d'une part les infractions qui sont commises par le biais d'un *système d'information et de communication* de celles qui l'ont pour objet[49]. Cette distinction se comprend en ce qu'elle permet de rendre compte de toute l'ingéniosité des cybercriminels dans leur quête inextinguible de profit ou de déstabilisation.

15.- S'agissant de la blockchain, laquelle est moins un système d'information et de communication qu'une plateforme de transactions ou de stockage, la distinction peut, semble-t-il, s'appliquer. Elle représente en effet un outil, neutre par nature, mais potentiellement nuisible dans ses effets et dont l'usage malveillant peut servir à commettre l'infraction. Les opérations réalisées sur cette chaîne de blocs sont certes soumises à des procédés de vérification par des tiers indépendants. Toutefois, la blockchain n'étant qu'une technique au service de diverses applications, elle peut constituer l'instrument indirect de l'infraction. Il n'est qu'à penser que celle-ci constitue la technologie sous-jacente des crypto-monnaies pour comprendre les risques qu'elle induit. Ces actifs désormais très répandus sont au confluent d'usages variés qui, s'ils sont pour la plupart licites,

[48] Selon un rapport du 5 décembre 2019 publié par Global Blockchain Market, le marché de la blockchain évalué à environ 1.4 milliards de dollars en 2018 devrait atteindre 53.5 milliards de dollars en 2028.
[49] GROUPE DE TRAVAIL INTERMINISTÉRIEL SUR LA LUTTE CONTRE LA CYBERCRIMINALITÉ, Rapport sur la cybercriminalité, février 2014.

peuvent cependant être frauduleux, voire criminels[50]. Aussi, il est fondamental de comprendre que la blockchain est un puissant vecteur pour la commission d'infractions **(CHAPITRE 1)**

Mais au-delà de son aspect instrumental, la blockchain est une structure. Plus précisément, il s'agit d'une structure décentralisée qui mobilise la puissance de calcul de plusieurs centaines, voire milliers, d'ordinateurs. Ce faisant, elle est nécessairement tributaire d'une interface extérieure qui lui permet de se déployer dans l'espace numérique. Cette matérialité indirecte de la blockchain en constitue le point de faiblesse. C'est par là que les cybercriminels pourront s'y attaquer dans le but d'en détourner l'usage. Par conséquent, il conviendra d'envisager la blockchain comme objet de l'infraction **(CHAPITRE 2).**

Chapitre 1. La blockchain comme moyen de commission de l'infraction.

16.- Parce que la notion d'infraction est en elle-même imprécise, il importe d'en préciser l'acception. Définie comme une *"action ou omission expressément prévue par la loi, qui la sanctionne par une peine en raison de l'atteinte qu'elle constitue à l'ordre politique, social ou économique[51]",* elle correspond donc à la violation d'une norme préexistante. Or, dans le cas de la cybercriminalité, il apparaît parfois difficile de trouver un fondement légal susceptible de recouvrir des actions par nature impalpables et dématérialisées. S'agissant de la technologie blockchain, la difficulté se double d'une absence de cadre normatif suffisamment étoffé eu égard à sa récente apparition. Face à ces apories, le législateur est souvent impuissant. Ainsi, c'est aux juges - et notamment aux juges du fond - de pallier l'absence d'incrimination ad hoc. Pour cela, ils pourront tout d'abord se fonder sur les qualifications dites de droit commun qui existent en dehors de la blockchain mais dont la commission est facilitée par ce vecteur **(Section 1)**.

[50] Selon le rapport FATF (2021), Opportunities and Challenges of New Technologies for AML/CFT, FATF, Paris, France, le pourcentage de transactions frauduleuses réalisées au moyen d'un actif numérique oscillerait entre 0,64 et 9,9 de l'ensemble des transactions réalisées par le biais de ces actifs. Parmi ces transactions, la criminalité est donc variable selon les estimations mais néanmoins réelle.
[51] Dictionnaire Larousse.

Par ailleurs, la place grandissante des dispositifs que la blockchain rend possible obligera le juge à les appréhender au regard de leurs spécificités. Il s'agira alors de prendre en compte leur dynamique de fonctionnement et les finalités qu'ils poursuivent. Aussi, ce sont des infractions propres à la blockchain qu'il s'agira d'envisager dans un second temps **(Section 2).**

Section 1. Les infractions de droit commun facilitées par l'usage de la blockchain

17.- Classiquement[52], le législateur établit entre les personnes et les biens une summa divisio qui irrigue tous les pans du droit en général et du droit pénal spécial en particulier. En somme, il n'est pas impensable de reprendre cette distinction dans le cadre de la criminalité permise par la blockchain. En effet, dans le cadre de la criminalité de droit commun, elle peut contrevenir à l'intégrité physique et psychique des personnes en facilitant les transactions portant sur des activités dangereuses à leur encontre **(Paragraphe 1)**

De même, et plus directement encore, les infractions de droit commun contre les biens seront potentiellement favorisées par cette technologie en ce que l'utilisation qui en est faite est encore peu saisie par le droit, si bien que de nombreux agissements peuvent s'y commettre et porter atteinte aux biens. Seront donc abordées dans un second temps les atteintes aux biens de droit commun facilitées par la blockchain **(Paragraphe 2)**

[52] La summa divisio reprise au sein du Code pénal de 1992 entre les atteintes aux personnes (Livre II) et les atteintes aux biens (Livre III) existe depuis le Code pénal de 1810 qui distinguait les "crimes et délits contre les personnes" (Chapitre premier du Titre II de la troisième partie) des "crimes et délits contre les propriétés" (Chapitre second du Titre II de la troisième partie).

Paragraphe 1. Les infractions contre les personnes

18.- La blockchain est le fondement technologique des crypto-monnaies. Or, ces dernières sont un moyen de paiement privilégié des criminels qui officient sur le Darkweb, espace de non droit où les infractions contre les personnes peuvent être organisées (A). Par ailleurs, ces actifs numériques sont acceptés ou exigés par certains individus en tant que contrepartie à la commission ou à la cessation d'une infraction (B)

A. Darknet, crypto-monnaies et atteintes aux personnes, une équation à plusieurs inconnues

19. - Le Darknet. Initialement créé pour les acteurs gouvernementaux, les journalistes, les militants des droits de l'Homme ou les lanceurs d'alerte[53], le Darknet ou Dark Web est un vecteur majeur d'infractions. Doté d'une double anonymisation[54] des connexions - par le biais de routeurs tels que TOR[55] - et des transactions par le recours à des pseudonymes et l'utilisation de monnaies virtuelles dont la plus célèbre est le bitcoin, il ouvre la voie à une criminalité dissimulée particulièrement difficile à endiguer.

20.- Le bitcoin constitue la crypto-monnaie la plus usitée sur le Darknet[56]. Il constitue le moyen de paiement des transactions réalisées sur le "marché" que représente cette partie cachée d'Internet. Ce "darkmarket" permet d'acheter ou de vendre tout type de produits qui ont pour point commun d'être attentatoires à l'intégrité des personnes. Les principales transactions portent sur des substances illicites telles que les stupéfiants (1) ou des objets illégaux telles que les images à caractère pédopornographique (2).

---

[53] A. JOMNI, "Le Darknet est-il une zone de non droit ?" , Sécurité globale, 2018/3 (N° 15), p. 17-23

[54] ibid.

[55] *"The Onion Router, désigné par l'acronyme Tor, est un réseau d'anonymisation permettant l'accès aux services cachés du darknet mais également au Web visible. Techniquement, il est constitué par des groupes de serveurs exploités par des bénévoles afin de garantir aux utilisateurs un accès plus sécurisé à des contenus cachés et une protection accrue de leur vie privée grâce à un anonymat quasi complet",* in N. OUCHENE*, L'applicabilité de la loi pénale à l'endroit de la cybercriminalité dissimulée* préc.

[56] Europol (2021), Cryptocurrencies - Tracing the evolution of criminal finances, Europol Spotlight Report series, Publications Office of the European Union, Luxembourg aux termes duquel le bitcoin représente 44 % des crypto-actifs utilisés.

1. Le trafic de drogue sur le Darknet, l'exemple de la plateforme Silkroad

21. - Un marché de la drogue florissant. Le trafic de stupéfiants et les infractions qui lui sont connexes[57] constituent des atteintes à l'intégrité physique des personnes[58]. Dans son rapport annuel sur la criminalité liée aux crypto-monnaies[59], l'entreprise privée Chainalysis évalue à 1,8 milliards de dollars le marché de la drogue sur le Darknet. Ce dernier profite en effet du très fort anonymat qu'offrent les crypto-monnaies dans le cadre des achats ainsi que la difficulté qu'ont les forces de l'ordre à appréhender les auteurs qui agissent en général depuis l'étranger. Cet anonymat est par ailleurs renforcé par l'usage de la technique du *mixage.* Il s'agit pour les acheteurs de mettre en commun leurs actifs, lesquels seront regroupés au sein d'un portefeuille unique dédié à cet effet. Ce portefeuille par lequel seront effectuées les transactions brouillera l'origine des fonds et rendra d'autant plus difficile la remontée de l'émetteur. La crypto-monnaie agit donc comme un vecteur facilitant les transactions sur le Darknet. Les marchés de la drogue sur ce support sont d'ailleurs très développés et représentent à eux seuls 60 à 70 % des sites selon Europol[60]. A titre d'illustration, il est permis de rappeler l'affaire *Silk Road*, du nom de l'un des sites de vente de drogue sur Internet les plus importants de l'histoire.

22. - Silkroad, un marché ou un système ? Fondé en 2011 par l'Américain Ross Ulbricht, la plateforme Silkroad a compté à son apogée près de 4000 vendeurs et plus de 150 000 clients[61]. Bien que non limitée à la vente de stupéfiants, il s'agissait cependant de son cœur de commerce. Le fonctionnement d'une telle plateforme et sa pérennité - démantelée en 2013, elle a permis la réalisation d'un million de transactions pour un gain compris entre 700 000 et 1,4 millions de bitcoins[62]. Cette prospérité de deux années d'un trafic de stupéfiants - alors qu'en général, un point de deal est fermé chaque jour en France[63] - rend compte des enjeux que représente l'adaptation des compétences et des techniques d'enquête en matière de suivi des réseaux de trafiquants et de saisie des crypto actifs[64].

---

[57] Il s'agit ici des crimes et délits en lien avec le trafic tels que les homicides ou les trafics d'armes.
[58] Les infractions de trafic de stupéfiants situées dans une section 4 (Du trafic de stupéfiants), du chapitre II (Des atteintes à l'intégrité physique des personnes), du Titre II (Des atteintes à la personne humaine), du Livre II (Des crimes et délits contre les personnes).
[59]The 2022 Crypto Crime Report, Chainalysis, 2022.
[60] D'après un article paru dans le journal Les Echos, "Drogue et dark web : la face sombre des crypto monnaies", 7 juin 2021.
[61] N. OUCHENE préc.
[62] ibid
[63] E. MACRON, cité dans le journal Le Point du 5 mai 2021, consulté le 20 décembre 2022.
[64] Voir la deuxième partie relative à la lutte contre la criminalité blockchain.

2. La pédopornographie sur le Darknet, un fléau avéré

23. - La pédopornographie désigne comme son nom l'indique l'ensemble des activités qui placent les mineurs au cœur de pratiques sexuelles rémunérées et corrélées à des traitements inhumains ou dégradants. Elle se déploie dans le monde physique mais également et surtout dans le monde virtuel où elle est facilitée là encore par l'anonymat et l'extraterritorialité des protagonistes. Le Darknet en constitue donc une caisse de résonance inquiétante. Les "consommateurs" des images ou vidéos à caractère pédopornographique utilisent bien souvent les crypto-monnaies à l'instar de l'achat de stupéfiants. Ces faits sont saisis par le droit pénal par l'article 227-23 alinéa 2 du Code pénal qui dispose que *"le fait d'offrir, de rendre disponible ou de diffuser une telle image ou représentation, par quelque moyen que ce soit, de l'importer ou de l'exporter, de la faire importer ou de la faire exporter"* est puni de cinq ans d'emprisonnement et 75 000 euros d'amende. Il s'agit donc d'une infraction par nature virtuelle qui trouve dans le Darknet un support idéal. Or, la qualification de cette infraction ne pose pas de difficulté d'interprétation quand est accomplie sur le Darknet une offre ou une acquisition d'images ou de vidéos à caractère pédopornographique par un individu en échange de monnaies virtuelles. Il s'agit donc d'un mode particulier de commission de l'infraction qui ne remet pas en cause son aspect originel. Mais à l'instar du trafic de stupéfiants, il pourra être particulièrement délicat de remonter la trace des acteurs de cette criminalité cachée. Cependant, des exemples de détection et de sanction de sites de vente pédopornographiques[65] par les autorités permettent de penser que l'adaptation de la répression est en cours et que l'impunité de ces réseaux sera à terme plus relative. Par l'usage même de la blockchain, il a ainsi été possible aux enquêteurs de remonter jusqu'au créateur de *Welcome to Video*, un site à caractère pédopornographique, et de découvrir son identité. Pour ce faire, ils ont utilisé la blockchain comme registre de transactions infalsifiable[66].

Au regard de ces deux exemples, le Darknet incarne à lui seul une source de criminalité exploitant l'une des potentialités de la blockchain : sont anonymat. Toutefois, parallèlement à ces espaces criminogènes et organisés, la crypto-monnaie et donc la blockchain peuvent être exploitées par des individus, isolés ou agissant en groupe, aux fins de porter atteinte à l'intégrité physique des personnes.

[65] L.H Newman, "How a Bitcoin Trail Led to a Massive Dark Web Child-Porn Site Takedown", *The Wired,* 16 octobre 2018 (consulté le 22 octobre 2022)
[66] Cette technique d'investigation innommée sera abordée dans la partie relative aux poursuites.

B. L'utilisation de la crypto-monnaie comme contrepartie de l'infraction

24. - Virtualité ou réalité de la criminalité blockchain. Au-delà des exactions commises sur le Darknet, les crypto-monnaies peuvent également servir de moyen de paiement dans le cadre d'une criminalité réalisée dans le monde réel. La valorisation de certaines de ces monnaies virtuelles et notamment le bitcoin[67] accroît leur usage éventuel dans le cadre de transactions criminelles diverses. Pour saisir l'émergence ou la potentialité de ce phénomène, il est possible de prendre en exemple le cas du "mandat criminel 3.0" (1) mais surtout le fléau des rançongiciels (2)

1. Des mandats criminels 3.0

25. - Des bitcoins contre un assassinat. L'article 221-5-1 du Code pénal introduit par la loi du 13 juin 2001[68] dispose que *"Le fait de faire à une personne des offres ou des promesses ou de lui proposer des dons, présents ou avantages quelconques afin qu'elle commette, y compris hors du territoire national, un assassinat ou un empoisonnement est puni, lorsque ce crime n'a été ni commis ni tenté, de dix ans d'emprisonnement et de 150 000 euros d'amende".* Il s'agit donc de réprimer l'instigateur proposant des fonds à un tiers afin qu'il commette une infraction qualifiée crime sans pour autant être passé à l'acte de manière à caractériser un fait de complicité. S'il n'apparaît a priori pas lié à l'univers de la blockchain, il peut y être rattaché dès lors que les avantages promis ou offerts à l'exécutant le sont en crypto-monnaies et qu'au surplus, la prise de contact entre le client et le prestataire de service se fait par le Darknet. Le cas du site Assassination Market[69] est topique des possibilités que recèlent ces actifs virtuels. Ce dernier établissait en effet une sorte de cagnotte abondée par des dons anonymes en crypto-monnaies et au moyen de laquelle devaient être rémunérés celles et ceux qui acceptaient d'accomplir la mission d'éliminer une personnalité désignée. Il s'agissait donc d'un système décentralisé par lequel tout individu pouvait commettre l'assassinat en échange d'un paiment en bitcoins. Ainsi, 40 bitcoins étaient offerts pour le meurtre du président américain Barack OBAMA et près de 125 pour celui du directeur de la Réserve fédérale américaine Ben BERNANKE. Là encore, le paiement se faisait par le biais de *mixer* et devait aboutir en pratique à la non-traçabilité des transactions.

---

[67] Malgré une forte baisse de sa valeur, le bitcoin est encore valorisé à 15 863 dollars (au 26 décembre 2022) selon le site bitcoin.fr.

[68] Loi n° 2001-504 du 12 juin 2001 tendant à renforcer la prévention et la répression des mouvements sectaires portant atteinte aux droits de l'homme et aux libertés fondamentales.

[69] A. GREENBERG, "Meet The 'Assassination Market' Creator Who's Crowdfunding Murder With Bitcoins", Forbes.com, 18 novembre 2013, consulté le 12 décembre 2022.

26 .- Même si ce site a été démantelé depuis lors, l'idéologie qu'il incarnait n'a pas disparu. Son concepteur poursuivait l'objectif d'éliminer l'élite politique et économique du pays qu'il accusait d'être à l'origine des maux de la société. Cette aspiration civilisatrice et émancipatrice est l'une des revendications les plus partagées par les utilisateurs de la blockchain en général et des crypto-monnaies en particulier. Cependant, cette finalité politique est souvent occultée par une recherche de profit comme le montre l'essor des attaques par rançongiciel.

2. Séquestration et crypto-monnaies

27. - Constitue un acte de séquestration *"le fait, sans ordre des autorités constituées et hors les cas prévus par la loi, d'arrêter, d'enlever, de détenir ou de séquestrer une personne, est puni de vingt ans de réclusion criminelle*[70]*".* La séquestration est donc un crime puni de vingt ans de réclusion criminelle si la victime n'a pas été volontairement libérée avant le septième jour par ses ravisseurs[71]. Si le texte ne précise pas l'objet de la rançon, celle-ci peut par conséquent prendre autant de forme que l'imagination des criminels le permet.

28. - Or, depuis quelques années, la "tendance[72]**" est de demander le paiement de ces rançons en crypto-monnaies, et plus précisément en Monero**[73]. Ce mode de paiement est bien entendu avantageux par l'anonymat et donc la protection qu'il offre aux criminels. Il requiert de la part des victimes l'ouverture d'un portefeuille ainsi que l'achat de crypto-monnaies ce qui implique pour celles ayant des difficultés avec Internet de solliciter un tiers et de révéler sa situation. A titre d'exemple, la femme d'un riche homme d'affaires norvégien, disparue en octobre 2018, a fait l'objet d'une demande de rançon de 10 millions de dollars en Monero en juin 2019. La police norvégienne lui a interdit de payer cette somme et il n'y a pas aujourd'hui encore, de nouvelles sur le sort de cette femme dont les chances d'être en vie sont faibles.

---

[70] C.pén., art. 224 -1.
[71] ibid. al.3
[72] J. MARTINON, Phénomènes criminels célèbres ou exotiques dans le champ des crypto-actifs, par J. Martinon, p. *534*
[73] Le Monero est une crypto monnaie à anonymat renforcé qui repose sur un processus d'authentification appelé signature par cercles : procédé cryptographique permettant à une personne de signer électroniquement de façon anonyme un message au nom d'un cercle. Un observateur ne voit que la signature du cercle sans pouvoir déterminer qui a réellement signé, définition issue du site Cryptoast.fr.

Paragraphe 2. Les atteintes aux biens

29.- Les atteintes aux biens facilitées par la blockchain sont très diverses. Elles peuvent concerner toutes les infractions d'appropriation frauduleuse en substituant la monnaie virtuelle à la monnaie classique. Néanmoins, dans le champ de ces infractions, certaines se démarquent de par leur ampleur et leurs effets délétères. Tel est le cas des attaques par rançongiciel (A) et de l'escroquerie (B).

A. Le ransomware : attaque informatique aux effets matériels

30. - Les rançongiciels. Phénomène croissant[74], dont les retentissements médiatiques et politiques dépassent parfois l'ampleur réelle, les attaques par *rançongiciel* ou *ransomware* constituent une menace latente pour les infrastructures, privées comme publiques. Lorsqu'elles portent atteintes à des établissements de santé, c'est la vie des patients qui est directement menacée par la paralysie parfois prolongée des systèmes informatiques. De même et plus généralement, c'est l'activité économique du pays qui est directement mise en péril[75]. Ces attaques sont également problématiques en ce qu'elles font généralement intervenir des réseaux structurés et organisés qui fournissent tous les éléments nécessaires à leur perpétuation. Du logiciel de pénétration dans le système vendus en ligne, aux mécanismes de blanchiment, en passant par la mise à disposition de portefeuilles, tout se déroule sur le Darknet sans qu'aucun contact physique ne soit requis. Ce paramètre complexifie d'autant plus le travail des enquêteurs. Aussi, face à cette épidémie[76], il est nécessaire de comprendre quel rôle jouent les crypto-monnaies et partant, comment se déroulent les différentes phases du *ransomware*.

31. - Le déroulement d'un ransomware. Les phases distinctes d'une attaque par rançongiciel sont désormais bien identifiées[77]. En effet, plusieurs étapes sont nécessaires pour aboutir à l'exigence

[74] "*57 % des entreprises déclarent avoir connu au moins une cyber-attaque en 2020"* selon 6ème Baromètre de la cybersécurité des entreprises du Club de sécurité de l'information français datant de février 2021.
[75] Agence nationale de sécurité des services informatique (ANSSI), *Guide des attaques par rançongiciel, tous concernés,* août 2021.
[76] Communiqué de presse, "Face à l'ampleur de la menace, l'ANSSI et le ministère de la Justice publient un guide pour sensibiliser les entreprises et les collectivités territoriales", 4 août 2020 : "*depuis le début de l'année, l'ANSSI a traité 104 attaques par rançongiciels"*
[77] Politique de sécurité: analyses du CSS, "Rançongiciels: approches nationales de protection", No 297, Février 2022

d'une rançon. Tout d'abord, le ou les auteurs de l'attaque vont devoir infiltrer le réseau de l'infrastructure, c'est-à-dire, son intranet ou son système d'exploitation. Pour ce faire, ils disposent de plusieurs techniques d'infiltration du système. La plus répandue est le *phishing*[78] qui consiste en l'envoi d'un lien par le biais d'un support quelconque - courrier électronique, sms, publicité etc. - qui va installer le virus lorsque l'utilisateur l'ouvrira. Ce virus va alors contaminer le système et aboutir à sa paralysie par le cryptage des informations. Enfin, et pour obtenir la clef de déchiffrement, les criminels vont exiger le paiement d'une rançon en crypto-monnaie - le plus souvent en bitcoins même si d'autres monnaies sont plébiscitées en raison de leur anonymat renforcé à l'instar de monero - vers un portefeuille dédié à cet effet et qui leur permettra par la suite de facilement blanchir le produit de leur infraction. Le paiement de la rançon n'offre cependant pas la certitude aux victimes de récupérer l'intégralité de leurs données et les pouvoirs publics ainsi que l'ANSSI exigent même que ces dernières ne paient pas[79]. Mais le silence gardé par les victimes qui souhaitent ainsi préserver leur réputation de sécurité et de fiabilité alimente un important "chiffre noir". L'ampleur du phénomène s'en trouve donc minimisée.

Pour pallier cette aporie, le projet de loi d'orientation et de programmation du ministère de l'Intérieur (LOPMI) envisage, en son article 4 de créer une assurance visant à couvrir les *"pertes et dommages causés par une atteinte à un système de traitement automatisé de données mentionnée aux articles 323-1 à 323-3-1 du code pénal est subordonné au dépôt d'une plainte de la victime auprès des autorités compétentes au plus tard soixante-douze heures après la connaissance de l'atteinte par la victime[80]".*

32. - La qualification des attaques par rançongiciels. La matérialité des attaques par rançongiciel peut faire s'interroger le juge sur la qualification idoine. En effet, si la cible est un système de traitement automatisé des données (STAD), il semble pertinent de recourir à la qualification spéciale d'atteinte aux STAD[81]. Or, ces incriminations pourraient aussi être appréhendées par le prisme de l'incrimination d'extorsion dont l'article 312-1 du Code pénal dispose qu'il s'agit *"d'obtenir par violence, menace de violences ou contrainte soit une signature, un engagement ou*

[78] Cette technique représenterait 80 % des attaques par rançongiciel selon le 6ème baromètre de la cybersécurité des entreprises publié en février 2021 par le Club de la sécurité de l'information français, in Rapport d'information fait au nom de la délégation aux entreprises relatif à la cybersécurité des entreprises, par MM. Sébastien MEURANT et Rémi CARDON, Sénateurs le 10 juin 2021.

[79] *"Il est recommandé de ne jamais payer la rançon. Son paiement ne garantit pas l'obtention d'un moyen de déchiffrement, incite les cybercriminels à poursuivre leurs activités et entretient donc ce système frauduleux. De plus, le paiement de la rançon n'empêchera pas votre entité d'être à nouveau la cible de cybercriminels",* Agence nationale de sécurité des services informatique (ANSSI), *Guide des attaques par rançongiciel, tous concernés,* août 2021 préc.

[80] Projet de loi adopté par la commission mixte paritaire le 1er décembre 2022.

[81] C.pén., art. 323-1 et suivants.

une renonciation, soit la révélation d'un secret, soit la remise de fonds, de valeurs ou d'un bien quelconque". L'extorsion vise donc l'hypothèse d'une contrainte exercée - qu'elle soit physique, par la violence ou morale, par la menace - afin d'obtenir de la victime qu'elle remette des fonds. Dans le cas des attaques par rançongiciel, la victime - souvent une personne morale de droit privée ou de droit public - est obligée de payer la rançon en échange de la libération de ses données. À défaut, elle s'expose à les voir être supprimées ou altérées. Dès lors, il s'agit bien d'une extorsion si elle s'exécute et d'une tentative si elle ne paie pas la rançon comme cela lui est imposé. Comment trancher entre ces qualifications en concours ?

33. - La jurisprudence de la chambre criminelle du 15 décembre 2021 permet de répondre de manière simplifiée. En effet, au terme d'un raisonnement constructif, elle décide de revenir sur sa position traditionnelle datant de 2016 et posant comme principe que "*des faits qui procèdent de manière indissociable d'une action unique caractérisée par une seule intention coupable ne peuvent donner lieu, contre le même prévenu, à deux déclarations de culpabilité de nature pénale, fussent-elle concomitantes*[82]*".* Elle retient désormais que "*outre la situation dans laquelle la caractérisation des éléments constitutifs de l'une des infractions exclut nécessairement la caractérisation des éléments constitutifs de l'autre, un ou des faits identiques ne peuvent donner lieu à plusieurs déclarations de culpabilité concomitantes contre une même personne lorsque l'on se trouve dans l'une des deux hypothèses suivantes : Dans la première, l'une des qualifications, telle qu'elle résulte des textes d'incrimination, correspond à un élément constitutif ou une circonstance aggravante de l'autre, qui seule doit alors être retenue. Dans la seconde, l'une des qualifications retenues, dite spéciale, incrimine une modalité particulière de l'action répréhensible sanctionnée par l'autre infraction, dite générale*[83]*".* Ainsi, le principe est en l'état actuel de la jurisprudence, celui du cumul idéal des qualifications en concours à une triple exception. Seuls seront exclus les cumuls entre infractions incompatibles, spéciales et générales et constitutives l'une de l'autre. Dans le cas du cumul entre les atteintes aux STAD et l'extorsion, il ne semble pas y avoir d'incompatibilité - les atteintes aux STAD ne sont pas exclusives de l'extorsion - ni de concours entre une qualification générale et spéciale - l'extorsion n'est pas une forme générique des atteintes aux STAD qui sont circonscrites à certaines formes d'infractions - ni même d'élément constitutifs commun - la Cour de cassation se montrant très exigeante sur cette condition en ne la retenant que lorsque l'une des infractions reprend nominativement dans ses éléments constitutifs ceux de l'autre

[82] Cass. Crim., 26 octobre 2016, pourvoi n° 15-84.552
[83] Cass. Crim., 15 décembre 2021, pourvoi n° 21-81.864.

infraction. Les juges pourront ainsi retenir les deux qualifications en respectant les règles de cumuls plafonnés des peines de même nature[84]. Finalement, la solution sera laissée à l'appréciation souveraine des juges du fond qui choisiront en fonction de l'opportunité. En ce sens, la restriction du mécanisme d'assurance prévu par la LOPMI aux seules infractions qualifiées d'atteintes aux STAD amène à penser que, si cette dernière est maintenue, elle incitera les autorités judiciaires à se tourner vers ces qualifications plutôt que l'extorsion.

B. De nouvelles formes d'escroquerie

34. - L'escroquerie est une infraction fondée sur la tromperie. Elle consiste pour son auteur à user d'un faux nom, d'une fausse qualité ou de manœuvres afin de convaincre sa victime de lui remettre des fonds, valeur ou encore un bien quelconque[85]. Elle peut donc emprunter différents visages et passer par une multiplicité de modalités. La blockchain en est une dont il faut préciser les contours.

35. - La Pyramide de Ponzi au service des cybercriminels. "L'escroquerie à la Ponzi" est une figure topique des escroqueries faisant intervenir plusieurs victimes. Il s'agit pour son ou ses auteurs de créer une entreprise - au sens économique du terme - donnant l'apparence de la rentabilité sur le temps long. Un produit est ainsi présenté comme offrant un fort rendement afin d'attirer les investisseurs. Progressivement, les fonds affluent et permettent de rémunérer les premiers arrivants avec des taux hors de proportion avec la réalité des systèmes financiers. Cependant, la Pyramide est un jour vouée à s'effondrer dès que les demandes de remboursement ne sont plus couvertes par des investissements suffisamment abondants. Dès lors, il n'est reste plus pour son concepteur qu'à se retirer avec la trésorerie amassée. C'est ainsi que le célèbre homme d'affaires Bernard MADOFF à escroqué pour près de 68 milliards de dollars sur 48 ans[86].

36. - L'attrait pour les crypto-monnaies offre de nouvelles formes d'escroquerie. En raison de leur forte volatilité, ces actifs alimentent en effet les spéculations les plus risquées. En réaction, les criminels profitent du flou entourant ces monnaies virtuelles et de leur relative méconnaissance par les investisseurs pour proposer des investissements à rendement élevé dans une nouvelle

[84] C. pén., art. 132- 3.
[85] C.pén., art. 313-1.
[86] "J.-G. DEGOS et J.-Y. DEGOS, "Chaînes de Ponzi et théorie des catastrophes : le point de non-retour des réalités financières", *La Revue du Financier*, mars 2017

crypto-monnaie ou un jeton non fongible[87]. À ce titre, une escroquerie fondée sur les Initial Coin Offerings (ICOs) a pu être découverte en Chine sur la plateforme "PlusToken". Les ICOs sont des jetons non fongibles émis par le biais de la blockchain. Ils sont générés ex nihilo et peuvent être acquis par le biais de monnaies légales ou virtuelles. Dans le cadre d'une escroquerie telle que celle organisée par la plateforme PlusToken, les victimes étaient invitées à se porter acquéreurs de jetons émis en échange de bitcoins ou d'ethereums. Classiquement, les organisateurs de cette opération n'ont jamais fourni la contrepartie de ces apports et se sont envolés après avoir obtenu près de deux milliards de dollars[88]. Cette forme d'escroquerie, dénommée *rug-pull,* constitue un phénomène d'ampleur et représentent pour l'année 2021 près de 7, 7 milliards de dollars détournés, soit une hausse de 82 % par rapport à l'année 2020[89].

37. - Les difficultés que pose cette forme d'escroquerie sont multiples. Eu égard à l'absence de décisions jurisprudentielles en droit interne, plusieurs interrogations quant à sa qualification et aux poursuites se font jour.

38. - Il s'agit tout d'abord de la détermination de l'objet pouvant être remis. Si le texte vise les *"biens quelconque"* et que la jurisprudence de la chambre criminelle se montre ouverte quant à leur acception - en admettant que l'escroquerie porte sur un service[90], des codes d'accès confidentiels à Internet[91] ou bien encore des primes et subventions de collectivités locales[92]- la question peut se poser de savoir ce qu'il en sera pour les crypto-monnaies remises dans le cadre d'un investissement. Or, il est désormais acquis que les crypto-monnaies entrent dans la catégorie des biens meubles incorporels[93]. Ce faisant, elles devraient être appréhendées comme telles par les juges du fond.

39 - Les poursuites sont également sujettes à des adaptations pour saisir le caractère anonyme et souvent extraterritorial des escroqueries[94]. Comme le développera la partie relative aux poursuites pénales, la compétence de la loi pénale pourra se résoudre au moyen de textes dérogatoires au principe général de territorialité[95] ainsi que par la prise en compte du caractère

---

[87] A. El Mejri, "La pyramide de Ponzi"*, Revue de Droit bancaire et financier* n° 4, Juillet 2020, étude 11
[88] *www.scmp.com/news/asia/australasia/article/3016604/six-chinese-nationals-wanted-beijing-internet-scam-arrested*, in A. El Mejri, "La pyramide de Ponzi", préc.
[89] Rapport Chainalysis : « Crypto-crime 2022 »
[90] TGI Lyon, 18 juin 1970.
[91] TGI Paris, 16 décembre 1997.
[92] Crim. 21 oct. 1991, n° 90-85.123
[93] *M. Bali, "*Les crypto-monnaies, une application des blockchain technologies à la monnaie" *: RD. bancaire et fin. 2016, étude 8, spéc. n° 14 in* A. EL MEJRI, préc.
[94]A. EL MEJRI, préc.
[95] C.pén., art. 113-2-1.

complexe de l'infraction permettant de saisir l'un de ses éléments constitutifs commis sur le territoire français[96]. L'enjeux sera donc d'identifier cet acte au moyen le cas échéant de techniques d'enquête adaptées[97].

Section 2. Les infractions propres à la blockchain

40.- Après avoir envisagé les leviers qu'offrait la technologie blockchain dans la commission d'infraction de droit commun pouvant être réalisées sans son intermédiaire, il importe désormais de présenter la criminalité qui lui est inhérente ou du moins qui lui est intimement liée. Il s'agit de produits dérivés de la blockchain, soit qu'elle en constitue le vecteur comme pour les NFT (**Paragraphe 1**) soit qu'elle en permette le fonctionnement comme le métavers (**Paragraphe 2**).

Paragraphe 1. L'aspect criminogène des NFT

41. - Les jetons non fongibles sont comme leur nom l'indiquent uniques. Ils peuvent ainsi être valorisés en fonction de leur rareté et de la demande qu'ils suscitent. Ils sont de plus générés par la blockchain ce qui rend leur production autonome et décentralisée. Par conséquent, cette dernière n'est soumise à aucun contrôle étatique. Ces deux caractéristiques renforcent l'attrait pour les NFT, lesquels peuvent, comme précédemment évoqué, être produits et commercialisés sur le marché légal. Mais elles en constituent également les failles par lesquelles les criminels peuvent s'engouffrer à des fins malveillantes. L'aspect criminogène des NFT se divise ainsi entre leur production (A) et leur échange (B).

A. La production des NFT comme source de criminalité

42. - Un NFT est généré par un smart contract[98], c'est-à-dire *"une application ou un programme qui fonctionne sur une blockchain[99]".* Cette technique permet donc de générer des jetons de manière automatique après en avoir programmé les modalités dans un smart contract. C'est donc par l'action

[96] C.pén., art. 113-2 al 2 : *"L'infraction est réputée commise sur le territoire de la République dès lors qu'un de ses faits constitutifs a eu lieu sur ce territoire".*
[97] Confère partie II.
[98] J. PROST et A. JEAN-BAPTISTE, " Les Non-fungible tokens saisis par le droit", *Dalloz IP/IT,* 5, mai 2022, p. 260-267
[99] https://academy.binance.com/fr/articles/what-are-smart-contract

d'un programme que naissent les NFT. Toutefois, malgré cette automatisation a posteriori, le programme est conçu a priori par une intelligence humaine, laquelle peut décider de donner à ces actifs une coloration illicite, notamment en falsifiant des oeuvres d'art (1) ou en incitant à la commission d'infractions à caractère terroriste (2).

1. La contrefaçon d'œuvres d'art

43. - Si chaque NFT est unique et est garanti comme tel par la blockchain, la liberté potentiellement illimitée de création de ces jetons fait naître le risque que ces derniers soient créés et vendus comme des œuvres d'art existantes. L'article L.335-2 du Code de la propriété intellectuelle précise que *"toute édition d'écrits, de composition musicale, de dessin, de peinture ou de toute autre production, imprimée ou gravée en entier ou en partie, au mépris des lois et règlements relatifs à la propriété des auteurs, est une contrefaçon et toute contrefaçon est un délit"*. L'article L. 335-3 du même Code ajoute que "e*st également un délit de contrefaçon toute reproduction, représentation ou diffusion, par quelque moyen que ce soit, d'une œuvre de l'esprit en violation des droits de l'auteur, tel qu'ils sont définis et réglementés par la loi*". Ainsi, le fait de créer un NFT identique à une autre œuvre peut constituer l'infraction de contrefaçon. Cependant, pour être caractérisée, la contrefaçon doit porter sur une *œuvre de l'esprit en violation des droits de l'auteur,* ce qui peut interroger quant à la qualification des NFT en tant qu'œuvre de l'esprit. Or, cette appellation ne saurait leur être applicable en ce qu'ils ne présentent aucune originalité[100] et qu'ils ne résultent pas d'un processus créatif[101], étant générés par un smart contract. Il serait donc nécessaire de réglementer les NFT afin de leur reconnaître le statut d'œuvre de l'esprit ou de créer une protection ad hoc.

2. Les NFT au service de l'idéologie terroriste

44. - Il est désormais établi que les organisations à caractère terroriste ont investi Internet pour recruter des candidats pour le djihad ou encore faire l'apologie ou la provocation au terrorisme[102]. À cet égard, les jetons non fongibles constituent un vecteur potentiel de la diffusion des thèses partagées par ces tenants de la terreur. Ainsi, selon une enquête du *Wall Street Journal*[103], des NFT

[100] C. ZERBIB et W. O' RORKE, "NFT : chaînon manquant ou maillon faible de l'art numérique", *Propr. ind,* 2021, n° 5, étude 11 in J. PROST et A. JEAN-BAPTISTE préc.
[101] M. TORELLI et G. HAAS, "Non-Fungible Token (NFT) : un outil efficace de protection des marques", *RLDA* 2021, n° 175.
[102] Voir à ce sujet K.BRISSAUD, *L'influence d'internet dans la radicalisation.* Droit. 2018.
[103] *Wall Street Journal*, "Islamic State Turns to NTFs to Spread Terror Message", 6 septembre 2022, consulté le 12 décembre 2022.

sous forme de carte auraient été émis à la gloire de l'État islamique en août 2022[104]. Bien que marginale, cette utilisation des NFT à des fins de propagande terroriste - qu'il s'agisse de terrorisme islamiste ou de terrorisme d'extrême-droite ou d'extrême-gauche - constitue une menace sérieuse pour les régulateurs d'Internet et plus largement les autorités publiques. En raison de leur caractère occulte et anonyme, ces formes d'apologie ou de provocation permettraient de contourner la censure traditionnelle et d'affermir dans l'esprit des terroristes en puissance les velléités de passage à l'acte. Il sera donc nécessaire de prendre en compte ce facteur dans le cadre des futures législations, ce que la Commission européenne s'est engagée à faire au travers de son projet de règlement MiCA[105], lequel sera présenté dans le cadre du chapitre consacré à la coopération européenne.

B. Les échanges de NFT face au délit d'initié

45. - Le caractère spéculatif des NFT. À l'instar des autres actifs numériques, la valeur des NFT n'est, en principe[106], pas fondée sur un sous-jacent concret tel qu'une devise ou une matière première. Dès lors, elle laisse libre cours aux spéculations à risque et peut parfois offrir des rendements spectaculaires pendant une brève période, avant qu'ils ne s'effondrent brusquement[107]. Or, là où il y a spéculation, il existe un risque que des individus disposant d'informations privilégiées en profitent pour fausser le libre jeu des marchés financiers et s'enrichissent ou enrichissent autrui de manière illicite. Il s'agit alors d'un délit d'initié réprimé par le Code des marchés financiers. Plus précisément, l'article L.465-1 du Code des marchés financiers sanctionne le fait pour une personne disposant d'une information privilégiée *"de faire usage de cette information privilégiée en réalisant, pour elle-même ou pour autrui, soit directement, soit indirectement, une ou plusieurs opérations ou en annulant ou en modifiant un ou plusieurs ordres passés par cette même personne avant qu'elle ne détienne l'information privilégiée, sur les instruments financiers émis par cet émetteur ou sur les instruments financiers concernés par ces informations privilégiées".* Cette incrimination a un champ d'application large en ce qu'elle englobe tout initié et vise aussi bien les opérations réalisées directement par celui-ci ou réalisée par

[104] M. FABRION, "Quand les groupes terroristes s'intéressent aux NFT", LesNumeriques.com, 6 septembre 2022, consulté le 12 décembre 2022.
[105] Proposition de Règlement DU PARLEMENT EUROPÉEN ET DU CONSEIL sur les marchés de crypto-actifs, et modifiant la directive (UE) 2019/1937.
[106] Il existe cependant des actifs numériques indexés sur d'autres valeurs et notamment les stable coins qui peuvent reposer sur le dollar ou l'or afin de réduire la volatilité des crypto-monnaies classiques.
[107] Ainsi et à titre d'illustration, la valorisation du bitcoin a atteint un record à 53 000 dollars l'unité le 15 novembre 2021 avant de retomber à 15 653 dollars le 26 décembre 2022 selon le site bitcoin.fr.

un tiers en raison d'une information obtenue de la part de cette personne. Quel lien peut-il être établi entre ce délit et les NFT ?

47. - Le développement des entreprises d'émission de NFT et l'absence de marché officiel pour ces actifs, sont une opportunité pour la commission de ce délit. Lorsqu'un jeton est émis par ces structures, il fait l'objet d'une "mise sur le marché" et son cours fluctue en fonction de l'intérêt qu'il suscite. Le choix de mettre en circulation tel ou tel NFT appartient à l'entreprise et ne doit pas être connu à l'avance sous peine de fausser la libre fixation du prix. Or, lorsque des personnes possèdent la connaissance de l'imminence de la mise en circulation d'un actif, elles peuvent aisément s'enrichir en anticipant une augmentation ou une diminution de son cours pour réaliser des investissements ou des reventes stratégiques. L'affaire OpenSea est un exemple topique de cette criminalité économique.

48. - OpenSea, une entreprise américaine de vente de NFT. Cette entreprise permet à ses utilisateurs de créer des NFT et de les proposer à l'achat sur le marché qu'elle leur ouvre. Selon le site Fortune, *"en février 2021 les ventes étaient l'équivalent de 95 millions de dollars US, en mars l'équivalent de 147 millions de dollars US, et en septembre à 2,75 milliards de dollars US"*. Toutefois, entre juin et septembre 2021, Nathaniel Chastain, ancien chef de produit chez OpenSea, aurait utilisé des informations privilégiées pour acheter des NFTs avant qu'ils ne soient mis sur le marché. Or, chaque mise sur le marché d'un actif s'accompagnant inexorablement d'une hausse importante du cours de ce dernier, il a pu s'enrichir de manière substantielle grâce à sa qualité d'initié. A la suite d'une enquête du FBI, il a été mis en accusation des chefs, notamment de délit d'initié[108].

Aussi, les jetons non fongibles sont également utilisés à des fins malveillantes. Ils créent les conditions permettant le développement de fraudes massives et sont les vecteurs de propagandes criminelles. Le déficit de régulation fait craindre une utilisation toujours plus grande dans ce type d'activité et met en lumière le retard pris par le droit face à des technologies disruptives. Il est donc fondamental de pallier ces lacunes en réhaussant le cadre législatif et réglementaire en vigueur.

[108] Department of Justice U.S. Attorney's Office Southern District of New York : "Former Employee Of NFT Marketplace Charged In First Ever Digital Asset Insider Trading Scheme", 1er juin 2022.

Paragraphe 2. Le Métavers, entre utopie et criminalité

49. - "*L'homme n'est ni ange ni bête, et le malheur veut que qui veut faire l'ange fait la bête*[109]". Cet aphorisme de Pascal s'applique également au Métavers. Ce monde virtuel destiné à améliorer les expériences sociales dans le cyberespace peut en effet servir de terreau aux activités criminelles diverses. Par son caractère immersif, il expose ses utilisateurs à des atteintes certes virtuelles mais aux effets somatiques réels. La notion de "personnalité virtuelle" retenue par le Conseil d'Etat dans son rapport sur Internet et les réseaux sociaux numériques[110] illustre cette connexité étroite entre l'existence de la personne et ses activités dans l'espace numérique. Dès lors, si le Métavers se veut être un monde virtuel, il est permis d'analyser les infractions qui sont susceptibles d'y être commises. Que celles-ci soient commise contre les personnes (A) ou contre les biens (B)

A. Des infractions commises dans le Métavers contre des personnes

50. - Métavers et blockchain ? Le Métavers peut reposer sur plusieurs dispositifs d'immersion tels que la réalité virtuelle - l'intégration d'éléments virtuels dans le monde physique par le prisme de technologies - ou la réalité augmentée - le développement maximal de l'intégration de l'agent dans le monde virtuel par l'apport de la 3ème, voire, 4ème dimension. S'agissant de la blockchain, et bien que celle-ci ne soit pas consubstantielle au fonctionnement du Métavers[111], elle en constitue cependant un support essentiel de par sa capacité à enregistrer et authentifier les transactions. Or, l'économie dans le Métavers, en l'absence d'intermédiaire dédié, est tributaire d'un tel système de certification. De plus, l'interopérabilité entre les différents univers, qui est une aspiration majeure de ses membres, est simplifiée par cette technologie qui permet notamment la persistance dans le temps et l'espace de ces métavers. C'est la raison pour laquelle la blockchain est pour l'instant nécessaire au Métavers.

51. - Des infractions contre les personnes. Dans le Métavers, les interactions sociales se font par la médiation d'avatars. Ces figures représentent les utilisateurs dans cet univers et peuvent revêtir des aspects variés, souvent très éloignés de ceux qu'ils incarnent. La conséquence de l'utilisation de la réalité augmentée ou virtuelle est que toute atteinte subie par l'avatar pourra être également

[109] B. PASCAL, *Pensées diverses III* – Fragment n° 31 / 85, 1678.
[110] Conseil d'État, *Internet et les réseaux sociaux numériques,* 2 juillet 1998.
[111] A.BASDEVANT C. FRANCOIS R. RONFARD, Mission exploratoire sur les métavers, octobre 2022.

ressentie par le représenté. La notion de violence morale telle qu'elle a été développée par la Cour de cassation[112], puis intégrée dans le droit positif, pourra être mobilisée[113]. Or, pourquoi refuser la qualification de violences à l'encontre de faits commis sur un avatar mais causant par leur intensité un vif choc émotif à la victime ?

De même, s'agissant des infractions à caractère sexuel, il est permis de s'interroger sur le fait de savoir si un acte de pénétration sexuelle ou une autre agression sexuelle commise sur un avatar pourra se voir qualifier pénalement de viol ou d'agression sexuelle. A cet égard, la doctrine est divisée. Certains[114] considèrent qu'il n'existe aucune raison juridique pour refuser la qualification d'agression sexuelle à l'encontre d'un avatar - et donc son utilisateur - commettant une telle agression contre l'avatar d'une autre personne. Il cite notamment l'exemple de la législation canadienne qui précise que *"une agression sexuelle est un geste à caractère sexuel, avec ou sans contact physique, commis par un individu sans le consentement de la personne visée ou, dans certains cas, notamment dans celui des enfants, par une manipulation affective ou par du chantage" (...),* ou encore le *"intentional infliction of emotional distress"* aux États-Unis qui permet aux victimes de comportements ayant provoqué chez-elles une profonde détresse de poursuivre leurs agresseurs sur ce fondement[115].

B. Les infractions commises dans le Métavers contre les biens

52. - Des atteintes contre les biens. Le Métavers est devenu un haut lieu d'échange et de transactions marchandes. Il est possible d'y acquérir des biens virtuels de toute sorte ainsi que des NFT par la monnaie qui est principalement le bitcoin. Se posent de facto des interrogations quant à la notion de propriété dans le Métavers, c'est-à-dire, de l'existence d'une propriété virtuelle[116]. Sa reconnaissance permettrait en effet de pouvoir qualifier les formes d'appropriation frauduleuses d'infractions contre les biens. Or, dans le cas du métavers fondé sur la blockchain, l'enregistrement des transactions assure une authentification et une garantie de propriété. Dès lors, il est possible de

[112] Cass. Crim, 4 juin 2019, pourvoi n°14-82.332 : "*Les faits de violences sont constitués, même sans atteinte physique de la victime, par tout acte de nature à impressionner vivement celle-ci et à lui causer un choc émotif*"
[113] C.pén., art. 222-14-3 : "*Les violences prévues par les dispositions de la présente section sont réprimées quelle que soit leur nature, y compris s'il s'agit de violences psychologiques".*
[114] T. VIALLAT, "Y a-t-il une justice dans la Métaverse ?", 25 septembre 2021 (consulté le 13 décembre 2022)
[115] Ibid.
[116] G. CHAMPAU,, "Second Life : un procès pour le droit de propriété virtuel », Numerama, 11 mai 2010 in "Les enjeux juridiques du Métavers : observations prospectives d'un phénomène en devenir !", blog avocat Deloitte, 3 juin 2022.

reconnaître des droits de propriété dans cet univers, lesquels pourront être méconnus par des acteurs malveillants.

53. - Le vol dans le Métavers. Le vol est la soustraction frauduleuse de la chose d'autrui[117]. Pour être établie, l'infraction doit donc porter sur la chose d'autrui. Il est donc au préalable nécessaire d'identifier le propriétaire de la chose soustraite. À défaut, l'appréhension d'une chose sans maître ne saurait caractériser l'infraction[118]. Dans le Métavers, la question posée est alors celle de l'existence d'une propriété. Or, il a été précédemment démontré que l'inscription des échanges effectués au sein de cet univers dans la blockchain permet d'authentifier le propriétaire actuel d'un bien virtuel. Aussi, en cas de soustraction frauduleuse de ce bien, l'infraction de vol pourrait être retenue. A cet égard, la Cour Suprême des Pays-Bas a condamné deux adolescents pour des faits de vol avec violence commis à l'encontre d'un autre adolescent. Les auteurs ont en effet exercé des pressions sur lui afin qu'il leur cède la détention d'accessoires dans le jeu en ligne *Runescape*, dans lequel les objets s'achètent et se revendent. Ils ont une valeur d'usage dans le jeu mais également une valeur marchande dans le monde réel et peuvent même être acquis aux enchères comme sur Ebay[119]. Dans l'affaire ayant donné lieu à condamnation, les deux adolescents ont forcé la victime à leur remettre ses actifs virtuels en le menaçant physiquement à son domicile avec un couteau[120]. Or, le Code pénal néerlandais et plus précisément son article 310 prévoit une telle condamnation à l'encontre de *"toute personne qui soustrait un bien quelconque appartenant en tout ou partie à une autre personne dans l'intention de se l'approprier frauduleusement".* A l'instar de l'incrimination française, il n'est aucunement fait mention d'une catégorie de bien particulière pouvant recouvrir celle des actifs virtuels présents dans le Métavers. Aussi, cette jurisprudence étrangère pourrait un jour être reprise en droit interne.

54. - L'univers métaphysique que représente le Métavers fait donc naître des enjeux tangibles s'agissant de l'adaptation des modalités traditionnelles d'enquête et de poursuite à un espace virtuel par nature globalisé. Ainsi, en ce qu'il ne peut être rattaché à un territoire en particulier - l'accès au Métavers pouvant s'opérer depuis tout endroit du monde via un ordinateur - il semble problématique de déterminer la loi pénale et la juridiction répressive compétentes en se fondant sur les seuls critères de territorialité. Il sera donc nécessaire de disposer de critères alternatifs pour

[117] C. pén., art. 311-1.
[118] Tel est le cas des choses communes qui n'admettent par nature aucun propriétaire comme la mer, le vent ou le gibier ainsi que des choses abandonnées dont le propriétaire initial s'est volontairement défait.
[119] Dutch Suprem Court, J. 10/00101, Criminal Chamber, January 31, 2012
[120] Ibid.

pallier cette lacune. De plus, l'interface que constituent les avatars entre l'infraction et leur dépositaire interroge sur l'existence et la nature du lien de causalité. Or, ce lien est essentiel s'agissant d'actes qui, par nature, sont commis sous le couvert de l'anonymat. Afin de respecter le principe constitutionnel de responsabilité personnelle[121], il est fondamental de pouvoir identifier avec précision l'auteur réel des atteintes, sauf à ce que le législateur prévoit un régime dérogatoire de responsabilité pénale, à l'instar de celle applicable en matière d'infraction de presse[122]. Enfin, seront nécessairement adaptés les actes d'investigations qui devront pouvoir appréhender les particularités de cet espace afin de récolter les preuves suffisantes.

Conclusion du Chapitre I

55.- Ainsi, la blockchain apparaît-elle comme devant être contrôlée en tant qu'elle est une source de commission d'infraction. Les fonctionnalités qui sont les siennes en font un instrument d'amplification des dommages et de diffusion rapide de la menace. Toutefois, il faut également la protéger dès lors qu'elle est susceptible d'être l'objet d'atteintes. Il s'agit en effet de l'une des ambivalences des nouveaux moyens de communication que d'avoir cette double qualité de vecteur et de cible. C'est donc cette deuxième face de la même pièce - ou crypto-monnaie - qu'il faudra envisager (**Chapitre II**).

Chapitre II. La blockchain comme cible de l'infraction

56. - La blockchain est également une structure. Même si elle n'est pas matérialisée par des dispositifs physiques de *hardware* - comme c'est le cas d'un ordinateur par exemple - elle est toutefois organisée en un réseau décentralisé qui forme le registre blockchain. Ce registre est alors inscrit dans la durée et accessible à tous les utilisateurs via leur clef publique. Ce faisant, cette accessibilité ouverte est source de failles pouvant être exploitées à des fins malveillantes. La blockchain est alors susceptible d'être prise pour cible en tant que telle et être attaquée dans sa structure (**Section 1**).

[121] Cons.const.,16 juin 1999, décision n° 99-411 DC.
[122] *Loi n° 82-652 du 29 juillet 1982 sur la communication audiovisuelle., art. 93-3.*

57. - Le contenu de la blockchain est potentiellement illimité. Résultant de la participation décentralisée de tous ses utilisateurs, il regroupe des informations diverses pouvant susciter l'intérêt des tiers. Or, bien que ce registre soit immuable en raison de son processus d'authentification qui fait intervenir plusieurs mineurs - dont au moins 51 % doivent intervenir pour valider un bloc[123] - il existe des techniques d'attaque informatique permettant de déjouer la relative immutabilité de la blockchain. Ainsi, c'est également le contenu de cette dernière qui peut être la cible d'atteintes (**Section 2**).

Section 1. Les infractions contre la structure de la blockchain

58. - La blockchain est-elle un STAD ? La qualification précise de la blockchain n'est pas une opération anecdotique. De ce travail réflexif préalable dépend en effet tout son régime, qu'il soit civil ou pénal. L'opération de qualification est *"un processus complexe par lequel les juristes décident ou non d'attribuer tel "nom" (catégorie juridique) à une chose ou à une situation (un fait), afin de leur associer des effets ou des conséquences juridique[124]"*. Il s'agit donc pour le juriste de déterminer l'appartenance de l'objet à qualifier à telle ou telle catégorie juridiquement établie pour lui appliquer le régime - l'ensemble des règles organisant son fonctionnement, son encadrement et sa protection - idoine. Dans le cas de la blockchain, cette opération peut se heurter à des difficultés tenant à sa relative insaisissabilité et à son caractère abstrait. Il n'existe en réalité pas une Blockchain mais des formes variables de blockchains. Par conséquent, il est permis de s'interroger sur la qualification à lui appliquer lorsqu'elle est notamment l'objet d'infractions pénales. À cet égard, une hésitation peut naître quant à la notion de système automatisé de traitement de données (STAD). Cette notion correspondant à une réalité précise peut-elle recouvrir la blockchain ? Dans le cas où la réponse serait affirmative, il sera pertinent d'appréhender les infractions contre la blockchain comme des atteintes aux STAD et en conséquence en observer le régime. Aussi, sera d'abord postulé que la blockchain est un STAD (**Paragraphe 1**). Dans le cas contraire, il serait nécessaire d'étudier ces infractions contre la blockchain en tant que structure *sui generis* et rechercher le cas échéant les incriminations qui sont les plus adéquates (**Paragraphe 2**).

[123] Pour qu'une transaction soit inscrite dans la blockchain, celle-ci doit être validée par plus de la moitié des mineurs ce qui représente 51 % de leur effectif. C'est pourquoi sera abordée l'attaque dite 51 %.
[124] V. CHAMPEIL-DESPLATS, *Méthodologies du droit et des sciences du droit*, Dalloz, 2014, p. 358.

Paragraphe 1. La blockchain considérée comme un STAD

59. - Qualification de STAD. Le professeur GASSIN précisait dans le répertoire Dalloz relatif à la fraude informatique[125] que la condition préalable pour caractériser une atteinte au STAD était la qualification préalable d'un tel système de traitement automatisé des données. Or, cette notion n'est pas définie par le Code pénal. C'est donc en dehors du Code qu'il faut en rechercher l'acception. À ce titre, lors de l'adoption de la loi du 5 janvier 1988 dite loi Godfrain[126], le Sénat retenait *"qu'on doit entendre par système de traitement automatisé de données tout ensemble composé d'une ou de plusieurs unités de traitement, de mémoires, de logiciels, de données, d'organes d'entrées-sorties et de liaisons, qui concourent à un résultat déterminé, cet ensemble étant protégé par des dispositifs déterminés[127]"*.

Ainsi, un STAD se compose selon cette définition de plusieurs éléments, matériels et logiciels, qui concourent tous - en symbiose - au traitement des données. Cette énumération non exhaustive[128] permet de retenir comme STAD tout ensemble de dispositifs liés entre eux, qu'ils soient physiques ou numériques et utilisés dans le cadre d'un traitement de données. Par exemple, ont pu être qualifiés de STAD le système carte bleue[129] ou le le réseau wifi[130]en ce qu'il *"permet de connecter par le vecteur hertzien des appareils de communication afin de les raccorder à un intranet ou à internet, est un système de traitement automatisé de données »*. S'agissant de la blockchain, il a précédemment été dit qu'elle pouvait remplir plusieurs rôles dont celui de permettre des actions automatisées par le biais des smarts contracts. En effet, en tant que support de ces contrats intelligents - dont il est possible de prévoir dans un protocole qu'ils accomplissent des tâches déterminées à l'avance - la blockchain revêt les fonctions d'un STAD. De plus, en ce qu'elle est constituée par un réseau d'ordinateurs agissant dans un but commun, elle représente a priori un "ensemble" au sens de la définition retenue par les sénateurs en 1988. Enfin, en raison de sa capacité de stockage des données, elle assume la dernière composante des STAD.

---

[125] R.GASSIN, Fraude informatique, *Répertoire de droit pénal et de procédure pénale,* Dalloz 1995 in F. CHOPIN, "Cybercriminalité", *Répertoire de droit pénal et de procédure pénale*, Dalloz 2020.
[126] Loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique
[127] Doc. AN 1987-1988, nº 1009
[128] F. CHOPIN, "Cybercriminalité" préc.
[129] TGI Paris, 25 févr. 2000
[130] C. FERAL-SCHUHL, *Cyberdroit*, 7e éd., 2018, coll. Praxis, Dalloz in F. CHOPIN, "Cybercriminalité"

D'ailleurs, l'assimilation du système bancaire à un STAD par la jurisprudence permet par une analogie - certes discutable en matière pénale mais néanmoins théoriquement soutenable - d'étendre cette qualification à la blockchain. Ses concepteurs ayant souhaité en faire une alternative au système bancaire, il est logique de lui offrir les mêmes garanties. Partant, la technologie blockchain sera tout d'abord appréhendée comme un système de traitement automatisé des données.

60. - Les atteintes aux STAD sont incriminées aux articles 323-1 et suivants du Code pénal. Elles recouvrent différents comportements qui tous ont pour cible ce système de traitement. Mais nonobstant cet objet commun, les modalités de commission de ces infractions sont distinctes. Elles concernent tant l'introduction et le maintien dans un STAD (A), que l'altération de son fonctionnement (B). Est également visée l'atteinte à l'intégrité des données contenues dans le STAD. Cette incrimination sera étudiée dans le cadre de la section 2 de ce chapitre relative aux infractions contre le contenu de la blockchain. De même, ne seront pas présentées les infractions satellites qui gravitent autour de ces atteintes principales en ce qu'elles ne présentent pas de spécificité s'agissant de la blockchain. En effet, tant la fourniture de moyens en vue de commettre une infraction contre un STAD[131]que la participation à un groupement formé en vue de la commission d'une atteinte aux STAD[132]correspondent à des infractions obstacles qui sont fréquemment érigées en droit pénal.

A. L'accès ou le maintien dans un STAD

***61.* - L'article 323-1, alinéa 1er, du code pénal** précise que « *le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende*[133] *».* Il s'agit tout d'abord de réprimer le ou les individus qui s'introduisent sans droit dans un STAD en sachant ne pas y être autorisés. Cette introduction n'est pas définie matériellement et seule l'absence de droit est exigée.

[131] C. pén., art. 323-3-1 : *"le fait, sans motif légitime, notamment de recherche ou de sécurité informatique, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre les faits prévus par les articles 323-1 à 323-3 du code pénal"*

[132] C. pén., art. 323-4 : " *la participation à un groupe formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou plusieurs infractions prévues aux articles 323-1 à 323-3-1"*

[133]Les peines sont portées à trois ans d'emprisonnement et 100 000 euros d'amende lorsque l'infraction prévue à l'article 323-1 a provoqué la modification ou la suppression des données contenues selon l'alinéa 2 et à cinq ans d'emprisonnement et 150 000 euros d'amende lorsque est concerné un système de traitement automatisé de données à caractère personnel mis en oeuvre par l'État selon l'alinéa 3.

S'agissant du maintien frauduleux, il peut suivre une introduction irrégulière ou régulière. Par exemple, la personne détentrice de droits d'accès qui se maintient au-delà de son habilitation en sachant ne pas y avoir droit, commet l'infraction. Pour analyser l'applicabilité de cette incrimination à la blockchain, il faut distinguer le type de chaîne de blocs dont il est question.

61. - S'agissant de la blockchain publique, une telle introduction ou un tel maintien serait difficile à caractériser en raison justement de son accessibilité libre de toute restriction. C'est d'ailleurs ce qui fait la force et la faiblesse de cette technologie : elle repose sur une collaboration décentralisée et désintermédiée avec le risque que cela suppose en termes de fiabilité et de licéité des données échangées ou enregistrées. L'infraction ne pourrait donc pas résulter d'un accès ou d'un maintien frauduleux en raison de l'absence de fraude. Ainsi, la qualification a pu être refusée dans le cas où un internaute avait accédé à une partie d'un site non autorisée mais en recourant à un logiciel de navigation grand public[134]. Par conséquent, pour pouvoir engager la responsabilité pénale de l'agent, il faudrait au préalable établir l'existence d'une condition d'accès à la blockchain, ou à l'un de ses éléments. Tel pourrait être le cas notamment dans le cadre des crypto-monnaies qui sont une illustration de la blockchain. Ces actifs numériques sont stockés sur des portefeuilles ou wallet. S'ils ne contiennent pas directement les crypto-monnaies, ils sont dépositaires des informations relatives aux clefs publiques et privées, elles même nécessaires pour opérer les transactions de crypto-monnaies[135]. La cible d'une atteinte aux STAD par accès ou maintien frauduleux pourrait plus particulièrement être la clef privée par laquelle un utilisateur de la blockchain peut accéder à sa crypto-monnaie : l'accès à la clef privée ouvre l'accès aux crypto-monnaies. Ainsi, commettrait une infraction au sens de l'article 323-1 du Code pénal, l'individu qui s'introduit sans droit dans un portefeuille. S'il s'empare de la clef privée d'autrui, il commet en sus une soustraction frauduleuse qui pourrait être considérée par les juges du fond comme un vol.

62. - Concernant la blockchain privée. Cette dernière se distingue de la blockchain publique en ce que son accès et son fonctionnement sont encadrés a priori par des règles. Qui plus est, elle est gérée par un gestionnaire identifié qui contrôle l'accès des participants en filtrant ceux qui doivent être approuvés. Dans une telle configuration, il serait possible de passer outre à cette barrière d'entrée et s'introduire ou se maintenir sans droit dans la blockchain, consommant de facto l'infraction d'accès ou de maintien illicite dans un STAD. À titre d'exemple, la blockchain Ripple est considérée comme privée : si toutes les transactions en ripple - qui est une crypto-monnaie - sont

[134] CA Paris, 30 octobre 2002 in F. CHOPIN préc.
[135] "Qu'est-ce-qu'un wallet crypto ?", Blog-wallet-crypto, 4 novembre 2021, consulté le 12 décembre 2022.

publiques, leur validation est centralisée et encadrée car les nœuds sont en nombre limité et choisis par l'entreprise Ripple Labs[136]. Dans un tel écosystème, il serait possible d'attaquer le système de traitement des données de l'entreprise opérant cette sélection afin de confisquer le choix des nœuds de transaction et ainsi contrôler la blockchain. Il s'agirait certes d'une atteinte indirecte à cette blockchain mais d'une atteinte réelle.

B. Atteintes à l'intégrité d'un STAD

63. - Aux termes de l'article 323-2 du Code pénal, est également pénalement réprimé *"le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données"*. Ce texte vise deux comportements distincts qui ont pour finalité commune de porter atteinte à l'intégrité du système. Ainsi, quel que soit le moyen employé, le STAD doit subir une altération effective. Cependant, bien que théoriquement différentes, ces deux modalités de l'infraction apparaissent en réalité uniformes. En effet, "*bien souvent, le juge recourt à la qualification d'altération du fonctionnement d'un STAD (C. pén., art. 323-1) plutôt qu'à celle de l'article 323-2 du code pénal, car le fait de fausser le fonctionnement implique son altération dans le but de produire un résultat différent de celui attendu[137]"*. Aussi, seule sera abordée l'entrave au fonctionnement d'un système de traitement automatisé de données dès lors qu'elle appelle les précisions les plus significatives.

64. - Le fait d'entraver le fonctionnement d'un STAD. Il s'agit ici de l'acte par lequel l'auteur de l'atteinte entrave le fonctionnement normal du système, lequel peut être dégradé, voire totalement compromis. La nature des attaques n'étant pas précisée, il semble possible d'imaginer tout type de moyen de nature à nuire au fonctionnement du système. Ainsi, l'attaque dite en *"déni de service distribué"* ou DDoS pour *Distributed Denial of Service Attack "vise à rendre inaccessible un serveur par l'envoi de multiples requêtes jusqu'à le saturer ou par l'exploitation d'une faille de sécurité afin de provoquer une panne ou un fonctionnement fortement dégradé du service[138]"*. Dans une blockchain, une telle attaque se conçoit aisément. En effet, le processus fondamental permettant l'exécution puis la validation d'une transaction repose sur la résolution par des mineurs de tâches complexes. Or, ces opérations de vérification demandent une grande puissance de calcul. Si les

[136] "Blockchain publique et blockchain privée : quelle est la différence ?" Cryptoast.fr, 29 novembre 2022, consulté le 10 décembre 2022.
[137] Op cit, F.CHOPIN.
[138] "Attaque DDoS, que faire ?" Cyber malveillance.gouv.fr, 9 octobre 2019.

mineurs constituant le réseau de nœuds sont confrontés à une forte sollicitation en matière de preuve de travail, ils pourraient être dépassés et, ainsi, ne pas parvenir à valider les transactions dans les temps. Cette altération du fonctionnement de la blockchain par saturation correspondrait ainsi à une attaque par déni de service distribué.

65. - Résilience de la blockchain face aux DDoS. Cependant, eu égard à son caractère décentralisé, la blockchain est très peu exposée à ce type d'attaque. Le nombre important de mineurs contribuant à valider les transactions diminue le risque de saturation individuelle en multipliant et répartissant la force de travail. C'est donc le particularisme de la blockchain qui la protège de telles attaques.

66. - Vulnérabilité de la blockchain face au crypto jacking. Le crypto jacking est un comportement malveillant par lequel l'auteur utilise l'ordinateur de sa victime à son insu et souvent de manière occulte, afin d'exploiter sa force de calcul dans le but de miner des crypto-monnaies. Selon Interpol[139], *"cela se produit généralement lorsque la victime installe involontairement un programme contenant des scripts malveillants qui permettent au cybercriminel d'accéder à son ordinateur ou à un autre appareil connecté à l'internet, par exemple en cliquant sur un lien inconnu dans un e-mail ou en visitant un site web infecté"*. L'appropriation par le criminel de l'ordinateur infecté afin de générer des crypto-monnaies constitue une double atteinte aux STAD. Il s'agit à la fois d'un accès et d'un maintien frauduleux dans un système de traitement automatisé de données - ici l'ordinateur - mais également une entrave au fonctionnement de ce STAD dès lors que son exploitation pour l'accomplissement du minage affecte sa capacité de traitement en général. Par conséquent, bien que la blockchain ne soit pas directement la cible de cette infraction, la crypto-monnaie usurpée est directement visée. Or, cette crypto-monnaie n'est qu'une application de la technologie blockchain.

[139] Interpol, "Crypto Jacking", septembre 2020.

Paragraphe 2. La qualification de STAD exclue

67. - La qualification relève du pouvoir souverain des juges du fond. En effet, "*il est possible que la qualification donnée par l'ordonnance du juge d'instruction, ou par la citation directe, soit modifiée par la juridiction à la lumière de faits nouveaux que le Ministère public ou le juge d'instruction avait ignorés et qui apparaissent au cours des débats. Mais, même si aucun élément nouveau n'est apparu, la juridiction de jugement n'est pas liée par la qualification donnée par le juge d'instruction ; elle peut estimer que, les faits étant les mêmes, le juge d'instruction ou la partie poursuivante s'est trompé et que la qualification exacte n'est pas celle qui avait été donnée*[140]*"*. Partant, la qualification initiale d'atteinte à un STAD peut être écartée au profit de celle d'une infraction plus générale. Ce choix peut être motivé par des considérations d'ordre juridique - absence des éléments constitutifs du STAD - ou d'opportunité - volonté d'appréhender un comportement sans avoir à caractériser au préalable un tel système. En tout état de cause, elle soulève la question des incriminations pouvant s'appliquer aux atteintes portées à la blockchain indépendamment de son assimilation à un STAD.

68. - La crypto-monnaie est peut-être l'application de la blockchain la plus exposée au risque criminel. En raison de leur qualification juridique incertaine et de leur forte valeur économique, ces actifs peuvent être l'objet de plusieurs formes de criminalité. Toutefois, afin de circonscrire l'étude de ces phénomènes, seront seulement présentées les infractions les plus prégnantes ou celles qui soulèvent les interrogations les plus vives. En effet, l'analyse statistique de la criminalité relative à la blockchain révèle qu'une forte proportion des infractions ont pour but de s'approprier des monnaies virtuelles. Dans son analyse de la criminalité pour l'année, l'entreprise Chainalysis estime à 3,2 milliards de dollars le montant des crypto-actifs volés en 2021[141], ce qui souligne les enjeux d'appréhender un tel phénomène. En outre, la nature juridique des crypto-monnaies fait naître des enjeux de souveraineté et de confiance dans l'institution monétaire en ce qu'elles se rapprochent des monnaies traditionnelles sans en revêtir tous les aspects. Cette ambivalence fait naître des risques d'atteinte à la confiance dans ces technologies. Ainsi, aux infractions d'appropriation frauduleuse

[140] G. LEVASSEUR, *Cours de droit pénal général complémentaire, "*La qualification", 1960.
[141] Rapport Chainalysis : « Crypto-crime 2022 » préc.

de la crypto-monnaie (A) succéderont les infractions portant atteinte à confiance dans ces crypto-monnaies (B).

A. Les infractions de soustraction frauduleuse de crypto-monnaies

69. - Le vol de crypto-monnaies s'impose à l'esprit de ceux qui cherchent à identifier les risques pesant sur ces valeurs virtuelles. Il s'agit en effet de l'infraction "classique" de soustraction frauduleuse qui, de par la brièveté de sa définition[142], est susceptible de s'appliquer à de nombreuses situations. Cependant, l'exigence de l'existence d'une "chose" soustraite amène à se poser la question de savoir si la crypto-monnaie est une chose pouvant faire l'objet d'un vol.

70. - La conception traditionnelle de la chose entendue comme un bien meuble corporel a rapidement laissé la place à une conception plus compréhensive de la jurisprudence. Dans une démarche dynamique d'interprétation téléologique[143], la Chambre criminelle de la Cour de cassation a multiplié les exemples d'extension de son acception de la chose objet du vol. Après avoir admis le vol de données par téléchargement sur le site de l'Agence nationale de sécurité sanitaire de l'alimentation, de l'environnement et du travail[144], elle a confirmé sa position en affirmant que *"le libre accès à des informations personnelles sur un réseau informatique d'une entreprise n'est pas exclusif de leur appropriation frauduleuse par tout moyen de reproduction[145]"*. Aussi, son application aux crypto-monnaies ne semble pas confrontée à un obstacle juridique infranchissable pour la jurisprudence et dépendra a priori de l'appréciation des juges répressifs, sous le contrôle de la Cour de cassation.

71. - L'objet du vol de crypto-monnaies doit cependant être précisé. En effet, ce ne sont pas directement ces actifs qui sont l'objet de l'infraction, ce qui les distingue des biens matériels. Ces derniers sont en réalité stockés sur des portefeuilles eux-mêmes accessibles par le biais d'une clef privée. Dès lors que les auteurs parviennent à se l'approprier, ils ont accès au portefeuille et aux crypto-monnaies qu'il contient. Les moyens mis en œuvre pour obtenir cette clef privée sont nombreux et reposent sur deux techniques principales que sont la falsification de la clef privée et

[142] C. pén., art. 311-1 : "Le vol est la soustraction frauduleuse de la chose d'autrui".
[143] F. DEBOVE, F. FALLETTI, I. PONS, *Précis de droit pénal et de procédure pénale*, Major, 2022, p.166, *"le modèle téléologique s'attache essentiellement à découvrir l'esprit qui a animé la genèse du texte. Non pas tant la volonté désuète d'un lointain législateur, mais l'intention hypothétique du législateur actuel"*
[144] Cass. crim., 20 mai 2015, n° 14-81.336.
[145] Cass. crim., 28 juin 2017, n° 16-81.113.

l'implantation d'un logiciel malveillant[146]. De plus, certains portefeuilles sont stockés sur un support physique tel qu'une clef USB[147]. Dans ce contexte, le vol de cette clef ne pose pas de difficulté de qualification : il s'agit de la soustraction d'un bien meuble corporel, paradigme de la chose au sens de l'article 311-1 du Code pénal.

72. - Qualifications concurrentes du vol. Si le vol est à même d'être retenu s'agissant de la soustraction de crypto-monnaies, d'autres incriminations peuvent être également applicables. Il en va ainsi des atteintes aux STAD précédemment évoquées dès lors que la soustraction de la clef privée est consécutive à l'introduction et du maintien de l'individu dans le portefeuille et que son appropriation peut porter atteinte à son intégrité[148]. C'est d'ailleurs ce qu'avait retenu la Chambre criminelle dans son arrêt de 2015[149] en admettant la double qualification de la Cour d'appel. Ainsi, seule l'absence préalable de caractérisation d'un STAD permettra de retenir la qualification de vol, ce qui, en termes d'effectivité de la réponse pénale, est un levier intéressant pour les juges.

B. L'atteinte à la confiance dans les crypto-monnaies

73. - La monnaie relève par nature de la souveraineté de l'État. Le droit de battre monnaie est en effet historiquement attaché à l'exercice de la puissance régalienne. Ce monopole a toujours été assuré par des incriminations érigées contre les faux-monnayeurs. Ainsi, dans *la section que le Code pénal [de 1810] consacre au faux (art. 132 à 165), un paragraphe 1er concerne la fausse monnaie » (art. 132 à 138), tandis qu'un paragraphe 2 traite de la « contrefaçon des sceaux de l'État, des billets de banque, des effets publics et des poinçons, timbres et marques » (art. 139 à 144)[150],* et l'auteur d'ajouter *"La monnaie joue un rôle considérable dans les sociétés modernes. Elle est le moyen de représenter la valeur des marchandises et des services et elle sert de référence à toutes les transactions ; elle traduit également la situation économique des divers pays et l'on sait avec quelle inquiétude ses fluctuations suivies par les gouvernements et les groupements financiers.*

[146]E. DEZEUZE et J. BIANCHI, "Le droit pénal des crypto-monnaies", *Revue de Droit bancaire et financier n° 3*, mai 2020, dossier 17

[147] "Questions à Olivier Le Guen sur la perquisition et la saisie des crypto-actifs" in Dossier : La justice pénale à l'épreuve des cryptomonnaies", *Dalloz IP/IT,* 2019.

[148] Il s'agirait donc d'une version aggravée de l'accès ou de maintien frauduleux dans un STAD conformément à l'article 323-1 alinéa 2.

[149] Cass. crim., 20 mai 2015 préc : *"Attendu qu'en l'état de ces énonciations, dépourvues d'insuffisance comme de contradiction, et d'où il résulte que M. X... s'est maintenu dans un système de traitement automatisé après avoir découvert que celui-ci était protégé et a soustrait des données qu'il a utilisées sans le consentement de leur propriétaire, la cour d'appel, qui a caractérisé les délits en tous leurs éléments, a justifié sa décision"*

[150]A.VITU, *Traité de droit pénal spécial,* "Le faux-monnayage", Paris 1982, T.I, p.490

Dès lors, on conçoit aisément que l'infraction de faux-monnayage puisse avoir de graves répercussions sur le crédit public et sur la confiance de chaque citoyen dans sa monnaie nationale". Dès lors, le faux-monnayage est une infraction qui porte atteinte à la confiance des citoyens. Confiance dans l'institution monétaire et par extension, confiance dans l'État censé en garantir la fiabilité. L'article 442-1 du Code pénal dispose ainsi que "*la contrefaçon ou la falsification des pièces de monnaie ou des billets de banque ayant cours légal en France ou émis par les institutions étrangères ou internationales habilitées à cette fin est punie de trente ans de réclusion criminelle et de 450 000 euros d'amende".* À la lecture de ce texte, toute forme de falsification ou de contrefaçon semble répréhensible à condition qu'elle porte sur des pièces de monnaie ou des billets de banque ayant cours légal en France.

74. - La crypto-monnaie est-elle une monnaie ? Les trois fonctions d'une monnaie sont, depuis Aristote[151], de faire office d'intermédiaire des échanges, d'être une unité de compte et une réserve de valeur. Face à cette définition, la crypto-monnaie peut être assimilée à une monnaie. Elle permet en effet d'effectuer des transaction - notamment mais non exclusivement, sur le Darknet - de constituer une unité de compte - un bitcoin permet de mesurer la valeur de la validation d'une transaction en rémunérant l'effort d'un mineur à hauteur de 6,25 bitcoins par bloc miné[152]- et une réserve de valeur - la spéculation sur les crypto-monnaies connaît un engouement important en raison de leur valeur parfois substantielle. Cependant, la qualification de faux-monnayage ne peut être, de lege lata, appliquée aux crypto-actifs en ce que ces derniers ne sont pas reconnus par l'État comme monnaie ayant cours légal. De même, *"la crypto-monnaie n'est ni émise ni garantie par une banque centrale ou une autorité publique étrangère"*[153].

75. - Qualifications envisageables. Est également réprimée "*la mise en circulation de tout signe monétaire non autorisé ayant pour objet de remplacer les pièces de monnaie ou les billets de banque ayant cours légal en France*[154]*".* Est ici visé le fait de créer un signe monétaire ayant pour objet de se substituer à une monnaie légale. Cette démarche se rapproche de l'idéologie de la blockchain animée par la volonté de s'extraire de la tutelle étatique en supprimant tout organe central. Cependant, l'article L. 54-10-1 du Code monétaire et financier issu de la loi PACTE précise, expressis verbis, que les actifs numériques ne sont pas une monnaie. Cela amène certains

[151] Aristote, *Politique*, livre I, IV[e] siècle av. J.-C.
[152] P.ANTHONIOZ, "Miner des cryptomonnaies pour gonfler son salaire, une promesse alléchante très risquée", Moneyvox.fr, 8 juillet 2022, consulté le 2 janvier 2022.
[153] E. DEZEUZE et J. BIANCHI, Le droit pénal des crypto-monnaies préc.
[154] C. pén., art. 442-4.

auteurs à conclure à l'exclusion des crypto-monnaies du champ d'application du faux-monnayage[155]. Cette position semble la plus cohérente car dans le cas contraire, cela signifierait que toutes les crypto-monnaies seraient potentiellement sujettes à incrimination, ce qui porterait une atteinte insurmontable à leur existence et par extension, aboutirait à leur dévaluation immédiate au préjudice des propriétaires.

Section 2. Les infractions portant sur le contenu de la blockchain

76. - La blockchain est également un support de l'information. Il s'agit d'ailleurs de l'une de ses caractéristiques principales. En ce qu'il s'agit *"d'une technologie de transfert et d'archivage d'informations permettant d'assurer un degré quasi parfait de fiabilité et de sécurité des transactions[156]",* la chaîne de blocs s'apparente à un registre ou un "grand livre" décentralisé. Cette propriété de stockage sécurisé est particulièrement importante dans le cadre des blockchains privées mise en œuvre par des entreprises pour échanger et conserver leurs données sensibles[157]. Toutefois, malgré le haut niveau de protection que confère à la blockchain son processus d'expansion[158], la malignité des criminels n'a d'égal que leur inventivité pour développer des techniques susceptibles de venir à bout de ces barrières. Dans cette situation, le contenu de la blockchain peut être compromis de deux manières. Ab initio, des données peuvent être frauduleusement inscrites et validées par l'action de véritables organisations criminelles. Celles-ci sont alors capables, selon les cas, de créer ou de modifier un ou plusieurs blocs de transactions non encore validés ou de faire valider un ou plusieurs blocs qu'elles ont intérêt à voir graver dans le marbre de la blockchain (**Paragraphe 1)**. A posteriori, et une fois le bloc définitivement enregistré, il est permis de se demander si les données qu'il contient sont réellement immuables et, le cas échéant, si cette immuabilité est conforme aux droits de la personne (**Paragraphe 2**).

---

[155] E. DEZEUZE et J. BIANCHI, préc.
[156] Op cit, M. QUEMENER, *Le Droit face à la disruption numérique,* p. 43.
[157] Ainsi de la "IBM Blockchain", destiné à "*permettre l'échange de données de confiance et l'automatisation des flux de travail au-delà des frontières grâce à la technologie du grand livre distribué et à la blockchain",* selon la présentation faite par le site internet https://www.ibm.com/blockchain.
[158] Voir *Introduction générale*, 5.2 sur l'immutabilité et l'intégrité de la blockchain.

Paragraphe 1. Les atteintes à la validité des transactions

77. - La validation d'une transaction repose sur la collaboration de plusieurs intervenants travaillant de concert. Ce processus est donc, par nature, à l'abri de toute monopolisation de la blockchain par des acteurs malveillants. Or, il existe des techniques informatiques permettant à un ou plusieurs acteurs de prendre le contrôle de la blockchain en s'accaparant des nœuds du réseau. Ces dispositifs sont variés et prennent la forme de véritables coups d'État contre la blockchain (A). En cas de succès, ils offrent à leurs exécutants des moyens d'instrumentaliser la blockchain à des fins criminelles (B).

A. Des coups d'État contre la blockchain

78.- Parmi les attaques ayant pour objet de préempter les transactions, il semble intéressant de présenter les plus fréquentes que sont l'attaque 51 % (1) et l'attaque Sybil (2).

1. L'attaque 51 %

79. - 51 % de la puissance de calcul développée par les mineurs, voici ce qu'il faut aux criminels pour devenir les maîtres d'une blockchain[159]. En effet, *"chaque transaction doit être vérifiées, validées et rassemblées dans des blocs, qui sont ajoutés par les nœuds à leur copie du registre lorsqu'ils sont certains que ces blocs sont valides. Pour faire en sorte que la* plupart des nœuds détiennent une même version du registre, *il convient que les nœuds parviennent à un consensus sur la validité des blocs de transactions[160]"*. Pour ce faire, il faut que la majorité des nœuds - animés par les mineurs - valide cette opération. Il s'agit donc d'une règle majoritaire qui est par principe atteinte par le consensus de plus de la moitié des mineurs qui ne sont pas liés entre eux. Or, dans le cas d'une attaque 51 %, une ou quelques personnes peuvent représenter ces 51 % en déployant une puissance de calcul égale ou supérieure à celle de la moitié des mineurs. Ce faisant, ils sont libres de *"créer des blocs plus rapidement que n'importe qui d'autre, et ainsi générer des blockchains à volonté[161]"*.

[159] Du moins dans les blockchains utilisant la technique de la preuve de travail qui est la plus usitée mais n'est pas la seule.
[160] F. G'SELL F. MARTIN-BARITEAU, L'impact des blockchains sur les droits de l'homme, la démocratie et l'État de droit, Rapport rédigé pour le Conseil de l'Europe, mars 2022, p. 7.
[161] Mcafee, "Rapport sur les menaces associées aux blockchain", 2018, p. 14.

80. - L'ampleur de certaines blockchains, et notamment celle du bitcoin, rend quasiment impossible une telle attaque. En effet, plus le nombre de nœuds et donc de mineurs est élevé, plus la puissance de calcul nécessaire pour atteindre 51 % l'est en retour. Les spécialistes parlent de *hashrate* ou *taux de hachage*[162] pour qualifier cette base de contributeurs. A contrario, pour les petites blockchains publiques ou les blockchains privées, le risque d'une telle attaque prend corps en raison du faible taux de hachage.

2. L'attaque Sybil

81. - Le terme Sybil est en réalité une homonymie. Il s'agit initialement du nom d'une patiente atteinte d'un trouble dissociatif de l'identité[163] du nom de Sybil DORSETT[164]. Il s'agit, appliqué à la blockchain, de la création par une même personne de plusieurs identités afin de tromper les autres utilisateurs. Plus précisément, l'auteur d'une telle attaque va *"contrôler plusieurs nœuds du réseau de façon à se présenter aux autres avec un grand nombre d'identités, toutes différentes*[165]*"*. Par cette définition, une telle attaque se rapproche des techniques usuelles de désinformation, notamment sur les réseaux sociaux, qui résultent d'une multiplication artificielle des comptes. Une fois ces nœuds contrôlés, l'individu peut agir avec une relative impunité et procéder à des actions malhonnêtes comme refuser de relayer des blocs ou ne relayer que ses propres blocs. À la différence d'une attaque 51 %, l'auteur ne prend pas le contrôle de la blockchain en surpassant les autres nœuds par sa puissance de calcul mais en multipliant les nœuds qui lui sont attachés. Il se heurterait par conséquent à une opposition de la majorité des autres nœuds si ces derniers se rendaient compte de sa manipulation, ce qui est difficile en pratique. Là encore, le risque d'effectivité d'une telle attaque dépendra du nombre de nœuds présents sur une blockchain.

---

[162] Ibid, p. 15.

[163] Selon le Manuel MSD, "*Dans le trouble dissociatif de l'identité, autrefois appelé trouble de personnalité multiple, deux ou plusieurs identités prennent tour à tour le contrôle d'une même personne. Par ailleurs, la personne ne se souvient pas d'informations qui sont normalement faciles à retenir, comme des événements de tous les jours, des informations personnelles importantes et/ou des événements traumatiques ou stressants"*.

[164] *Sybil* est un roman biographique de Flora Rheta Schreiber paru en 1973 aux États-Unis. Il traite de la thérapie d'une femme appelée Sybil Dorsett et diagnostiquée d'un *trouble dissociatif de l'identité* : tour à tour, seize personnalités différentes, possédant chacune leurs émotions et leur manière d'être, prennent le contrôle du comportement de cette femme. Le roman raconte donc la thérapie de cette femme (de son vrai nom Shirley Ardell Mason) in J. DUMAS,., P. LAFOURCADE, A. TICHIT & S. VARRETTE, (2022), "Qu'est-ce qu'une attaque Sybil ?" in *Les blockchains en 50 questions: Comprendre le fonctionnement de cette technologie*, Dunod, 2022, pp. 283-284

[165] Ibid.

B. L'instrumentalisation de la blockchain à des fins malveillantes

82. - Neutre par essence, la blockchain peut néanmoins devenir un puissant vecteur de criminalité. Parce qu'elle peut contenir tout type d'informations, et ce de manière définitive, la chaîne de blocs est susceptible d'être utilisée par des criminels afin de commettre leurs exactions (1). De plus, lorsqu'elle est contrôlée par un petit nombre d'acteurs, ces derniers peuvent procéder à des transactions irrégulières (2).

1. La blockchain, support potentiel de données à caractère criminel

83. - Selon une étude allemande[166], près de 99 % des données contenues dans des bitcoins sont des textes ou des images. Or, parmi ces images, certaines étaient en lien avec de la pédopornographie. Ce détournement de la blockchain n'est en soi pas surprenant tant les cybercriminels sont inventifs pour créer de nouvelles formes d'infractions traditionnelles. La pédopornographie étant un phénomène général dont les modalités de consommation évoluent au gré des nouvelles technologies, il semblait évident que la blockchain en constituerait l'un des vecteurs. En effet, les données stockées n'étant pas vérifiables car cryptées lors du processus de validation, elles ne font l'objet d'aucun contrôle a priori. Cela permet d'inscrire en toute impunité des images de cette nature. Les auteurs précisent[167] en outre que *"étant donné que 112 pays interdisent la possession de contenus pédopornographiques, que nombre de ces pays imposent d'autres restrictions interdisant la distribution de ce type de fichier, et que la nature décentralisée même du Blockchain rend tous les utilisateurs responsables du contenu répréhensible ajouté au Blockchain par d'autres",* et ce nonobstant la méconnaissance du contenu réel de la blockchain par ses utilisateurs. Cette complicité sans élément moral interroge les principes fondamentaux du droit pénal et soulève également des difficultés d'imputation de la responsabilité pénale eu égard à l'anonymat offert par la blockchain.

84. - La propagande en faveur du terrorisme consiste, aux termes de l'article 421-2-5 à *"provoquer directement à des actes de terrorisme ou de faire publiquement l'apologie de ces actes"*. Le texte n'apporte pas de précisions quant aux moyens employés à cette fin. Or, après le terrorisme 1.0 qui exploitait les médias pour diffuser son idéologie, le terrorisme 2.0 qui utilisait quant à lui les réseaux sociaux pour éviter le contrôle des services de renseignement[168], le terrorisme

[166] R. MATZUTT, J. HILLER, M. HENZE, J. H. ZIEGELDORF, D. MÜLLMANN, O. HOHLFELD, K. WEHRLE, "A quantitative analysis of the impact of arbitrary blockchain content on bitcoin", *Communication and Distributed System*s, RWTH Aachen University, Germany,
[167] Ibid,
[168] K. BRISSAUD, *L'influence d'internet dans la radicalisation.* Droit. 2018.

3.0 utilise désormais la technologie blockchain et ses dérivés. En effet, comme l'ont montré les développements sur l'aspect criminogène des jetons non fongibles[169], il est possible d'implémenter dans la blockchain du contenu à caractère terroriste ou faisant l'apologie de tels actes - qu'il s'agisse de textes incitant à la commission d'actes terroristes, d'images ou de vidéos violentes ou encore d'appel au don. Ce procédé - envisageable mais pour l'heure marginal - participe de l'engouement des terroristes pour les nouvelles techniques de l'information et de la communication dans la diffusion de leur idéologie et le recrutement de leurs disciples. Il soulève bien évidemment des enjeux majeurs en termes de prévention et de répression eu égard au caractère occulte dont peut être revêtue la blockchain.

2. La validation de transactions irrégulières

85. - Le problème des généraux byzantins et la double dépense. Une transaction en crypto-monnaie n'est définitivement achevée que lorsqu'elle a été validée et intégrée dans la blockchain. Durant ce laps de temps, un même individu peut donc transférer plusieurs fois la même unité à plusieurs destinataires différents et faire que cette monnaie soit, comme le chat de SCHRODINGER, virtuellement dans plusieurs portefeuilles à la fois. Cette double dépense peut être accidentelle et résulter de la problématique des généraux byzantins[170] qui ne peut être surmontée que si suffisamment de généraux sont loyaux. Dans le cadre d'une transaction, cette théorie correspond à la situation dans laquelle les acteurs loyaux de validation des transactions sont suffisamment nombreux pour ne pas compromettre la régularité de ces dernières. A contrario, lorsque la majorité des acteurs sont déloyaux, ils peuvent valider des transactions irrégulières et même effectuer plusieurs fois la même transaction : c'est la double dépense. Dans ce contexte, la majorité malveillante peut valider plusieurs transactions portant sur le même actif mais au profit de bénéficiaires différents. Ce faisant, *"l'attaque par double dépense permettrait de multiplier artificiellement une crypto monnaie tout en faussant le registre de la blockchain, enlevant toute crédibilité à cette dernière[171]"*. Or, à l'issue d'une attaque 51 % ou d'une attaque Sybil, le contrôle obtenu sur le processus de validation des blocs pourrait aboutir à cette irrégularité néfaste.

---

[169] Voir n° 27

[170] Selon Cointribune. com, "Qu'est-ce que le Byzantine General Problem", 3 octobre 2021, : "*L'origine de ce terme proviendrait, selon la légende, d'un groupe de généraux byzantins qui assiégeaient une ville ennemie. La seule façon pour eux de gagner était que les généraux planifient un plan de bataille commun afin d'unir leurs forces contre l'adversaire. Cependant, parmi ces généraux, certains étaient des traitres et travaillaient secrètement pour l'ennemi. Leur intérêt était alors de faire leur possible pour que le plan de bataille global ne fonctionne pas afin de permettre à la ville assiégée de s'en sortir".* Cette situation ne peut être surmontée que si suffisamment de généraux sont loyaux et s'assurent de la régularité des ordres.

[171] "Qu'est-ce qu'une attaque par double dépense sur la blockchain ?" Coin Academy.fr,

Paragraphe 2. Les atteintes aux données contenues dans la blockchain

86. - Les données sont devenues un actif à part entière sur le marché financier. La valorisation des plus grandes entreprises - et notamment des GAFAM[172] - repose désormais moins sur leurs biens matériels que sur les données qu'ils ont recueillies sur leurs utilisateurs. Dès lors, ces données représentent une cible de choix pour les cybercriminels. Elles peuvent être volées puis revendues sur le marché comme un bien de consommation. Or, parmi les fonctions assurées par la blockchain, il y a notamment celle de stocker des données. Cela constitue par conséquent un risque supplémentaire de criminalité à l'encontre de cette technologie. Deux situations sont envisageables. D'une part, les attaques peuvent porter sur les données appréhendées en tant qu'élément constitutif de la blockchain, analysée pour l'occasion comme un système de traitement automatisé de données (A). D'autre part, les informations personnelles que supportent ces données peuvent faire l'objet d'une atteinte à la vie privée en raison des caractéristiques mêmes de la blockchain (B).

A. Les données comme élément constitutif de la blockchain

87. - Un texte, trois comportements.[173] L'article 323-3 réprime "*le fait d'introduire frauduleusement des données dans un STAD, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient "*. Sont ici visés l'introduction de données, l'appropriation et l'exploitation des données ainsi que la suppression ou modification de celles-ci.

88. - L'introduction frauduleuse de données fait généralement suite à l'accès et au maintien dans un STAD. Il s'agit de toute adjonction ou modification des données contenues dans un système[174]. Appliquée à la blockchain, elle ne paraît possible qu'au stade initial de la transaction, c'est-à-dire, avant que le bloc ne soit validé. En effet, dès lors que le bloc est ajouté à la chaîne des blocs précédents, il ne peut plus être modifié et recevoir de nouvelles données.

89. - L'extraction de données afin d'en faire un usage ultérieur. *"Cette notion d'extraction permet de sanctionner celui qui réalise une simple copie de données qui demeurent à la disposition*

[172] Acronyme désignant Google, Apple, Facebook, Amazon et Microsoft.
[173] F. CHOPIN. *op.cit.*
[174] Tel fut l'une des qualifications retenues à l'encontre du trader Jérôme KERVIEL dans le cadre de sa condamnation pour abus de confiance à l'encontre de la société générale en ce qu'il avait introduit des données dans le système de trading de ladite société. (Cass. 19 mars 2014, n° 12-87.416).

de leur légitime propriétaire contrairement à la qualification de vol[175]*"* Toutefois, à l'instar du vol de crypto-monnaies, l'extraction de données contenues dans la blockchain ne peut se réaliser que par l'intermédiaire de la clef privée ouvrant l'accès à la transcription de ces données. En ce sens, il serait possible de concevoir une attaque portant sur le système sur lequel est conservée cette clef et tendant à en reproduire les informations permettant de décrypter le hash de transaction[176] et donc les données échangées et enregistrées. C'est un risque important pour les blockchains privées mises en place par des entreprises ou institutions et par lesquelles elles échangent et conservent des données sensibles. Aussi, un travail de prévention semble nécessaire.

90.- L'impossible modification ou suppression des données contenues dans la blockchain. In fine, le texte sanctionne le fait de supprimer ou de modifier des données. Or, si par principe l'élément matériel de cette infraction est assez simple à caractériser - modification ou suppression effective ou tentée des informations contenues dans un STAD tel qu'un site internet - le cas de la blockchain appelle encore une fois des précisions. En raison de son immutabilité, la chaîne de blocs ne peut être modifiée. Une fois le bloc, support des données, validé et horodaté, il sera visible par tous et nul ne pourra en changer la composition. La seule manière d'apporter une telle modification serait d'ajouter un bloc rectificatif à la blockchain, ce qui laisserait persister le bloc et ses données. Ainsi, le caractère intangible de cette technologie peut constituer une protection efficace contre ces atteintes aux données. Cependant, il peut aussi représenter un risque pour les données personnelles.

B. La blockchain comme risque pour les données personnelles

91. - La protection des données personnelles participe plus généralement du droit au respect de la vie privée consacré par l'article 8 de la Convention européenne des droits de l'homme et des libertés fondamentales[177]. Selon la Cour européenne des droits de l'homme : *"La protection des données à caractère personnel revêt une importance fondamentale pour la jouissance par une personne de son droit au respect de la vie privée et familiale, du domicile et de la correspondance, tel que garanti notamment par l'article 8 de la Convention*[178]*"*. Par conséquent, les données personnelles et le respect de la vie privée sont consubstantiels. Or, une fois inscrites sur la

[175] F. CHOPIN. *op.cit.*
[176] Sur la technique de cryptographie asymétrique, voir n° 3.
[177] CESDH., art.8 :*"Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance"*.
[178] Fiche thématique "Protection des données personnelles", Service de l'exécution des arrêts de la Cour européenne des droits de l'homme, septembre 2022.

blockchain, ces données sont sanctuarisées, immuables et accessibles. Cela pose donc des questions quant au respect de la vie privée par la blockchain elle-même.

92.- RGPD et blockchain. La confrontation de cette technologie au règlement européen sur la protection des données[179]suscite des interrogations multiples[180] . Ce texte, adopté sous l'égide de l'Union européenne, met en place un certain nombre d'impératifs dont la compatibilité avec le fonctionnement de la blockchain est plus que relative.

93. - L'identification d'un responsable de traitement exigé par le RGPD[181] afin de pouvoir lui soumettre un recours est rendue difficile, voire impossible par le caractère décentralisé de la blockchain. La désignation d'un tel responsable serait également pratiquement inenvisageable eu égard au nombre de blockchains différentes. Seules les blockchains privées pourraient répondre à cette exigence par le fait qu'elles sont gérées par une entité identifiée.

94. - Le droit à la modification ou à la suppression des données[182] est également compromis par le caractère intangible de la blockchain[183]. Il n'est en effet pas possible de modifier des données inscrites dans la blockchain. Comme développé plus haut, seul l'ajout d'un nouveau bloc afin de modifier les informations du bloc précédent est possible.

95. - La transparence relative de la blockchain. L'une des finalités poursuivies par la blockchain est de rendre les transactions transparentes et accessibles au plus grand nombre. En effet, toutes les transactions ainsi que les adresses utilisées sont visibles sans exigence particulière en termes d'accessibilité. Il est donc possible d'obtenir des informations sur les utilisateurs et ainsi porter atteinte à leur vie privée. Toutefois, la limite majeure à cette possibilité est que les transactions effectuées le sont sous le sceau d'une adresse publique correspondant généralement à un pseudonyme. Ainsi, l'identité réelle d'un utilisateur n'est jamais directement révélée. Il s'agit donc d'un risque relatif et en réalité limité.

---

[179] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE.
[180] Voir par exemple F. G'SELL F. MARTIN-BARITEAU, "L'impact des blockchains sur les droits de l'homme, la démocratie et l'État de droit", *Rapport rédigé pour le Conseil de l'Europe*, mars 2022.
[181] RGPD., art. 54.
[182] RGPD., art. 16.
[183]F. G'SELL F. MARTIN-BARITEAU, *op.cit.*

Conclusion du Chapitre II et du Titre I

96. - Au cœur de la blockchain se concentrent donc des puissances contradictoires, faites d'idéaux de progrès mais également de craintes substantielles. Elle incarne ce que Claude LEFORT appelait le "lieu vide du pouvoir[184]", en raison de sa relative insaisissabilité conceptuelle. Pouvant à la fois catalyser l'infraction mais également la subir, elle est l'outil a priori parfait pour servir à une criminalité se voulant de rupture. Mais au-delà de ce noyau dur, les enjeux criminogènes de la chaîne de blocs ne s'arrêtent pas à cette approche restrictive. Pour en saisir toute l'envergure, il convient d'étendre le champ d'analyse aux phénomènes qui gravitent autour de ce véritable instrument du crime (**Titre II**).

Titre II. L'utilisation de la blockchain aux frontières de l'infraction

97. - Comme tous les phénomènes sociaux[185], le crime s'est complexifié et mondialisé. Désormais, il se décompose en plusieurs étapes qui concourent in fine à la consommation de l'infraction. Or, au plus la criminalité se perfectionne, au plus elle requiert des moyens - matériels et humains - importants. Dans ce contexte, le cas du terrorisme s'impose avec acuité. En effet, bien que cette criminalité de la peur soit fondée sur une asymétrie entre le coût du passage et les dommages provoqués[186], elle est tributaire d'un financement massif et diversifié. Pour assouvir leurs besoins, les terroristes ont imaginé et continuent d'imaginer des méthodes disruptives et adaptées aux réponses des États. Aussi, la technologie blockchain pourrait être un nouveau vecteur de financement du terrorisme au regard de ses potentialités et ainsi être utilisée en amont du crime (**Chapitre I**).

98. - Assurer l'impunité des auteurs est l'autre enjeu de la criminalité. En effet, il ne saurait y avoir de passage à l'acte[187] sans une garantie ou du moins une espérance de pouvoir se soustraire à la justice des hommes. Pour atteindre cet état de paix, les groupes de criminels mettent en œuvre

[184] C. LEFORT, *Le Temps présent. Écrits 1945-2005,* Belin, 2007.
[185] E. DURKHEIM, *Les règles de la méthode sociologique* (1894), Paris, P.U.F., 14e édition, 1960, pp. 65-72].
[186] Selon le rapport publié par la Commission nationale sur les attaques terroristes contre les États-Unis du 11 septembre 2011, le coût de la préparation des attentats pour les terroristes aurait représenté entre 400 000 et 500 000 dollars alors que le coût estimé pour les États-Unis est évalué selon les sources, à environ 4000 milliards de dollars (voir à cet égard J. STIGLITZ, L. BILMES, *The Three Trillion Dollars War*, New York, W.W. Norton, 2008)
[187] Du moins de la part d'un individu rationnel et n'agissant pas sous le coup de l'émotion comme.

force ingénierie afin de blanchir le produit de leur crime ou le patrimoine qui provient de leur activité. Le blanchiment de capitaux, bien qu'il soit avéré depuis des décennies et appréhendé comme tel par les organes répressifs, ne cesse d'évoluer dans ces modes opératoires. La blockchain en est un dont il faut analyser les risques (**Chapitre II**).

Chapitre I. En amont : le financement du terrorisme

99. - L'élément matériel du financement du terrorisme met en exergue la volonté du législateur de donner à cette infraction une acception compréhensive. En effet, selon l'article 422-2-2 du Code pénal, *"constitue également un acte de terrorisme le fait de financer une entreprise terroriste en fournissant, en réunissant ou en gérant des fonds, des valeurs ou des biens quelconques, ou en donnant des conseils à cette fin (...)".* Les notions de fonds, valeurs et biens quelconques renvoient à la définition traditionnelle des infractions contre les biens[188]. Dès lors, il est permis de penser que l'appréciation des juges sera analogue à celle de ces infractions, même si des interrogations pourront apparaître s'agissant de la qualification de ces faits[189].

100. - Parler du financement du terrorisme au singulier n'est pas suffisant pour présenter cette infraction. Il est plus exact de parler des financements, tant les techniques utilisées varient au cours de l'histoire et selon les organisations terroristes. En effet, il serait difficile de dresser une liste exhaustive des moyens de financement utilisés par les groupes terroristes en raison de leur faculté d'adaptation à la réponse des autorités étatiques. L'identification et la suppression d'un flux financier aboutit systématiquement à l'apparition d'une nouvelle source de revenus. De même, le virage technologique emprunté par les terroristes leur permet d'exploiter les évolutions techniques pour en faire des leviers d'action. Aussi, les modalités "classiques" de financement du terrorisme devront être analysées à l'aune de leur modernisation par la blockchain (**Section 1**).

101. - Mais au-delà d'une simple modernisation des formes traditionnelles, le financement du terrorisme peut également être intrinsèquement lié à la blockchain et ses utilisations. Il s'agit ici de formes de financement inédites qui n'existeraient pas sans ce dispositif. Elles sont encore plus risquées car par nature peu ou méconnues. Partant, les modalités de financement inhérentes à la blockchain devront être évoquées (**Section 2**).

[188] Livre III, Titre I Code pénal.
[189] Voir les n° 106 à 108 relatifs aux difficultés de qualification soulevées par la blockchain.

Section 1. La modernisation des modes classiques de financement

102. - Le terrorisme est une notion imprécise. Désigne-t-elle une activité ou bien les acteurs qui la mettent en œuvre ? Si le terrorisme est traditionnellement une criminalité organisée et institutionnalisée au sein de groupements - Al Quaida, Daesh, Aqmi, Boko Haram etc. - il tend de plus en plus à s'individualiser et à se délocaliser. L'émergence croissante de "loups solitaires", ces "*individus radicalisés agissant seuls et choisissant eux-mêmes leurs cibles comme leur mode opératoire"*[190], fait naître des problématiques prégnantes pour identifier la menace et la prévenir. Au regard de ces deux formes de terrorisme, il est possible de distinguer deux types de financement : le financement du terrorisme et le financement des terroristes.

103. - Modernisation du financement du terrorisme. La blockchain constitue certainement un vecteur potentiel du financement du terrorisme. De par ses applications diverses et notamment la création et le transfert de crypto-monnaies, elle offre aux organisations terroristes - et donc au terrorisme en général - des moyens renouvelés de se financer (**Paragraphe 1**).

104. - Désintermédiation du financement des terroristes. Les auteurs d'acte de terrorisme sont - comme les mercenaires jadis rémunérés pour leur service - financés pour préparer et commettre leurs actes. Si la confiance est au cœur de leur rapport, alors la blockchain - dont le fonctionnement est fondé sur la confiance dans la technique - représente un mode anonyme et sécurisé de financement des terroristes (**Paragraphe 2**).

[190]H. MOUTOUH, *Dictionnaire du renseignement,* Paris: Perrin, 2018, pp. 517-518.

Paragraphe 1. Une conception renouvelée du financement du terrorisme

105. - Au faîte de leur puissance, certaines organisations terroristes ont pu s'apparenter à de véritables États dans l'État[191], disposant d'un territoire, d'une population, et d'un gouvernement. Or, comme tout État, le besoin de financement est récurrent. Afin d'alimenter leur arsenal, de former leurs soldats, de diffuser leur propagande ou de se projeter à l'étranger pour commettre leurs exactions, les groupes terroristes ont toujours dû pourvoir à leurs besoins. Pour ce faire, ils recourent principalement à des modes de financement extérieurs. Il s'agit en particulier de dons provenant de l'étranger. À cet égard, l'utilisation de la crypto-monnaie pour faciliter ces donations doit être soulignée (A). En outre, et afin d'assurer leur indépendance et leur résilience face à l'action menée par les États souverains - au premier chef desquels les États-Unis - ces organisations ont développé des moyens d'autofinancement. Là encore, ces formes traditionnelles pourront être analysées au regard de la blockchain (B).

A. L'économie terroriste du don au prisme de la crypto-monnaie

106. - Le financement étranger du terrorisme s'est développé durant la Guerre froide, au moment où des groupes terroristes étaient financés par des États dans le cadre de "guerres par procuration[192]". Depuis lors, les financeurs étatiques ont cédé la place à des entités ou personnes privées. Celles-ci contribuent désormais à la majeure partie des dons reçus par les groupes terroristes[193]. Ces dons se caractérisent par leur nombre important et leur faible montant. Ce faisant, ils sont susceptibles d'échapper aux radars des autorités de contrôle et ainsi être difficiles voire impossibles à déceler. Néanmoins, malgré la discrétion de ces transferts, l'adaptation des pouvoirs publics et l'amélioration des techniques d'identifications des flux financiers au travers de dispositifs de prévention[194]oblige les organisations à repenser leur modèle de donation. En effet, même si les envois de sommes d'argent se font par des méthodes rapides et discrètes - cartes prépayées,

[191] Ainsi de "l'État islamique" ou Daesh qui a pu à son apogée représenter 40 % du territoire irakien et 33 % du territoire syrien, selon Anne-Laure Vaurs-Chaumette dans "DAECH, un « État » islamique ?", In: *Annuaire français de droit international*, volume 60, 2014. pp. 71-89.
[192] V. BOYER et S. KRIMI, *Rapport d'information déposé par la Commission des affaires étrangères sur la lutte contre le financement du terrorisme,* Assemblée nationale, 3 avril 2019.
[193] Certains pays, dont la Syrie de Bachar al-Assad, sont accusés sur la scène internationale d'avoir financé des organisations terroristes.
[194] Voir les développements relatifs aux normes LCB-FT de la partie II.

paiements électroniques, services de paiement par Internet etc. - ils passent toujours par l'intermédiaire d'un prestataire identifié et contrôlable, ce qui les rend donc traçables. Le secteur bancaire formel est devenu trop dangereux pour les terroristes qui doivent donc y substituer d'autres modes de financement.

107. - La crypto-monnaie est-elle la forme parfaite de financement du terrorisme ? La question est légitime au regard de ses caractéristiques et des risques qu'elle induit en la matière. En s'affranchissant de tout intermédiaire, les transactions par le biais de crypto-monnaies peuvent devenir une forme de don quasiment intraçable et provenant de n'importe quel pays. Le "pseudonymat" qu'elles confèrent aux parties, s'il n'est pas un garant absolu d'impunité, permet aux échanges de passer sous les radars des autorités de contrôle. La décentralisation de la blockchain brouille l'origine et le destinataire des fonds, rendant d'autant plus difficile le travail des enquêteurs. La rapidité des transactions en crypto-monnaies est synonyme de leur multiplication et de leur imbrication dans un ensemble de flux financiers complexes à analyser. Enfin, l'immutabilité de ces transferts par le recours à la technologie blockchain est un gage de sécurité pour les groupes terroristes en ce qu'elle empêche toute rétractation de la part de l'émetteur et limite ainsi les pertes[195].

108. - De ces avantages offerts par la blockchain au financement exogène du terrorisme, les organisations ne semblent pas s'être saisies[196]. Plusieurs raisons peuvent expliquer cette réticence des terroristes. La technicité exigée pour l'utilisation à grande échelle de la blockchain n'a semble-t-il pas encore été maîtrisée par les groupes terroristes[197]Disposant souvent d'infrastructures vétustes et démunies en technologie, ces organisations pâtissent donc tout d'abord d'un manque de moyens matériels. Recrutant majoritairement des individus désœuvrés et déclassés socialement, les terroristes sont également en manque de moyens intellectuels et humains pour maîtriser cette technologie. Enfin, la forte volatilité des crypto-monnaies peut également ralentir leur développement dès lors que leur conversion en monnaie légale pourra être source de perte de valeur. Ainsi, seulement 4 % des fonds servant à financer le terrorisme auraient adopté la forme de

[195]A.BRILL, L. KEENE, "Cryptocurrencies : the next generation of terrorist financing ? ", *Defence Against Terrorism Review* Vol. 6, No. 1, Spring Fall 2014, pp. 7- 30.

[196] Les exemples d'appel au don en crypto-monnaies restent en effet marginaux. Ainsi, le 28 août 2015, ALI SHUKRI AMIN, un jeune homme de 17 ans, a été arrêté par les services du FBI après avoir expliciter sur un réseau djihadiste le fonctionnement des crypt-monnaies. Plaidant coupable, il a été condamné à 11 ans de prison en Virginie. Cette qualification de financement du terrorisme par la simple foruniture de conseil pour utiliser le bitcoin est révélatrice de l'interprétation extensive de cette incrimination par les autorité judiciaires américaines. Il n'est pas certain qu'elle telle qualification ait été retenue en France.

[197]J. SOLOMON-STRAUSS, "Terrorist Use of Virtual Currencies, Containing the Potential Threat", *Center for New American Security*, 3 mai 2017.

crypto-monnaies[198]. Mais, malgré une faible diffusion en l'état actuel, le recours à ces formes de dons est plus que plausible et doit éveiller la conscience des autorités de contrôle.

B. L'autofinancement du terrorisme renforcé par la blockchain

109. - Dualité de nature des flux financiers. L'autofinancement du terrorisme a pour particularité de mêler des flux licites et des flux illicites de revenus[199]. Il se compose en effet à la fois de fonds issus d'activités à caractère légales - exploitation minière, travaux publics, impôts[200] etc. - et d'autres de nature criminelle. En effet, l'une des particularités des groupes terroristes est que, en parallèle de leurs activités principales qui constituent en elles-mêmes des infractions pénales, ils commettent d'autres infractions pour se procurer des moyens d'action. Parmi elles, les trafics divers (1) et les formes d'appropriation frauduleuses (2) semblent devoir être appréhendées à l'aune de la blockchain.

1. Le trafic illicite générateur de crypto-monnaies

110. - Le trafic de produits illicites constitue une source importante de financement du terrorisme. Bien qu'il soit difficile d'évaluer la part qu'il représente dans l'économie terroriste, la diversité des produits sur lequel il porte amène à penser qu'il constitue une source majeure de financement[201]. Au trafic de stupéfiants s'ajoute le trafic d'armes, de biens culturels, d'espèces animales ou encore de ressources minières. Dans cette configuration, les groupes terroristes se rapprochent de la criminalité organisée.

111. - Un cyberterrorisme ? La crypto-monnaie est désormais une monnaie admise et plébiscitée pour les transactions illégales. L'instrument d'opacité que représente le Darknet offre en effet aux terroristes une plateforme sécurisée pour la revente des produits issus du trafic. Cette forme de financement pourrait d'ailleurs être qualifiée de cyberterrorisme. Entendu comme *"un acte*

---

[198] O. KHARIF, "Crypto Terrorism Funding Is Growing More Sophisticated", Bloomberg 17 janvier 2020 in H. BORDET et A. ILARI, "Cybermonnaies et terrorisme", note Université Côte d'Azur, mars 2021

[199] V. BOYER et S. KRIMI, *Rapport d'information déposé par la Commission des affaires étrangères sur la lutte contre le financement du terrorisme* préc.

[200] La mise en place d'un système d'imposition auprès des populations des territoires contrôlés est ici classé dans la catégorie des fonds d'origine licite malgré l'illégalité manifeste de son instauration pour le distinguer des flux illicites qui résultent d'infractions à part entière.

[201] Op cit, V. BOYER et S. KRIMI : "*Après une interruption de ces activités, les Shebab ont recommencé à tirer un revenu important du commerce de charbon de bois, sur lequel le groupe prélève des taxes. Ces revenus représenteraient aujourd'hui environ 10 millions de dollars par an, après avoir atteint des sommes qui auraient été jusqu'à 56 millions de dollars".*

terrorisme commis via Internet[202]*",* il s'agit de l'acmé de l'adaptation des terroristes aux nouvelles techniques de l'information et de la communication. Désormais, il est acquis que certaines organisations terroristes disposent d'une expertise suffisante pour utiliser Internet au soutien de leurs activités. Dans ce contexte, émerge le risque de voir se développer - à l'instar du site SilkRoad - des sites terroristes sur le Darknet mettant en relation acheteurs et vendeurs de produits illicites et utilisant la crypto-monnaie comme moyen de paiement.

2. Des appropriations frauduleuses de crypto-monnaies

112.- La crypto-monnaie pouvant faire l'objet d'une appropriation frauduleuse[203]**,** il existe un risque qu'elle le soit par des groupes terroristes aux fins de se financer - avec les limites exposées plus haut quant à leur volatilité. En ce sens, les vols ou extorsion de crypto-monnaies pourraient être poursuivis par les groupes les plus sophistiqués. Pour ce faire, les cyberterroristes pourraient recourir à une attaque par rançongiciel à l'instar d'autres groupes criminels et exiger leur paiement en actifs numériques. Pourraient aussi être envisagés des enlèvements contre rançons payées en crypto-monnaies, à l'instar de ce qui a pu être présenté au titre de la criminalité de droit commun[204] même si la pratique des enlèvements est en recul[205]. La difficulté pour ces groupes est notamment celle de se faire payer en crypto-monnaies, ce qui implique la création et la gestion d'un portefeuille dédié. Or, comme vu précédemment, cette étape supplémentaire dans le financement du terrorisme ne semble pas accueillir l'adhésion des organisations. À l'inverse, le financement d'individus isolés et expatriés par le recours à la blockchain pourrait être envisagé.

---

[202] Op. cit, N. OUCHENE.
[203] Voir notamment les développements sur le vol au n° 50.
[204] Voir n° 27 sur la séquestration.
[205] Selon l'entreprise Statista, le nombre d'enlèvement de nature terroriste serait passé de près de 15500 en 2015 à environ 4500 en 2020 disponible en ligne à l'adresse : https://fr.statista.com/statistiques/564079/terrorisme-enlevements-regroupes-par-pays-2007/

Paragraphe 2. L'efficience potentielle du financement des terroristes par la technologie blockchain

113. - L'une des menaces les plus fortes du terrorisme et sa globalisation. Il repose en effet sur des milliers individus disséminés dans le monde, partageant une même idéologie, sans pour autant être rattachés par un lien objectif de nationalité. Ainsi, les groupes peuvent-ils frapper depuis l'étranger en envoyant leurs émissaires ou en sollicitant les nationaux des pays cibles[206]. Pour pourvoir à ces attaques, ces derniers ont besoin de financement, certes de faible importance[207], mais qui leur assure une certaine autonomie d'action. Dès lors, parmi les techniques traditionnellement utilisées, la blockchain pourrait constituer une opportunité pour les loups solitaires. En ce sens, le procédé traditionnel de la hawala, reposant sur le recours à un tiers de confiance doit être analysé dans une dynamique fondée sur les particularités de la crypto-monnaie (A). En outre, ces actifs pourraient affranchir les terroristes de la nécessité de passer par un tel intermédiaire (B).

A. La relation de confiance au fondement de la "crypto-hawala"

114. - La hawala[208] répond au besoin d'assurer des transactions sécurisées dans des pays où les institutions financières sont défaillantes. Elle fut créée pour permettre aux diasporas des pays développés d'aider leurs proches restés dans leur pays d'origine. Le fonctionnement du mécanisme repose avant tout sur une relation de confiance. Lorsqu'un individu A situé dans un pays A veut envoyer de l'argent à un individu B situé dans un pays B, il charge un intermédiaire présent dans le pays A de prendre contact avec un intermédiaire du pays B. Ces deux *hawaladars*[209] vont alors entrer en relation pour le compte des deux parties. L'argent fourni par A sera envoyé par l'intermédiaire A à l'intermédiaire B lequel paiera directement le bénéficiaire B. Le paiement peut aussi se réaliser sans déplacement de somme d'argent et reposer sur un système de compensation entre les deux courtiers. Dans tous les cas, les intermédiaires reçoivent une commission pour le

[206] Ainsi, selon les chiffres du ministère de l'Intérieur cité dans un article du journal *Libération* en date du 29 avril 2021 et consulté le 2 janvier 2023, 78 % des auteurs d'attentats terroristes - aboutis et déjoués - étaient de nationalité française.
[207] Selon une étude du *Centre d'analyse du terrorisme*, les attentats du 7 janvier 2015 contre Charlie Hebdo et l'Hyper Casher auraient couté aux auteurs 25 800 euros dont 21 000 euros en armes et munitions cité dans *Le Parisien*, 17 octobre 2016, consulté le 12 décembre 2022.
[208] Terme arabe signifiant transfert.
[209] Terme arabe désignant l'intermédiaire.

transfert des fonds dont le montant varie. Grâce à ce système, les deux parties n'entrent pas en contact et peuvent même ne pas se connaître. La confiance réside exclusivement dans la bonne foi des intermédiaires. La valeur des transferts ayant comme vecteur la hawala est d'environ 500 milliards de dollars[210].

115. - Neutre par nature, une transaction par hawala peut bien entendu être dévoyée à des fins criminelles. En effet, dès lors que le paiement fait intervenir au moins deux intermédiaires qui peuvent être plus nombreux - la dilution du lien de causalité entre l'émission et l'infraction complexifie les poursuites. Cette technique a ainsi pu être utilisée pour financer ou blanchir le trafic de stupéfiants[211], ou encore, pour financer des attaques terroristes[212]. Il s'agit donc d'une figure dangereuse de financement dans son application criminelle qui pourrait être employée pour transférer des fonds aux terroristes expatriés.

116. - Pour se perpétuer, "*les hawalas ont su se réapproprier le système en s'adaptant à l'ère des nouvelles technologies de l'information et de la communication pour dépasser les contraintes de financement du système bancaire et les coûts que peuvent engendrer les règles qui régissent les institutions financières modernes[213]".* La question de l'effet de la blockchain sur le fonctionnement des hawalas est centrale. En effet, il est permis de penser que cette technologie pourrait être utilisée pour améliorer son efficacité et sa sécurité. Si le schéma classique passe par l'envoi d'une somme d'argent en liquide ou par virement, il est par extension envisageable de concevoir un paiement par crypto-monnaie. L'identité de l'émetteur serait alors inconnue à la fois par le bénéficiaire, mais également par l'intermédiaire. Cette double inconnue rendrait impossible toute identification de l'auteur du financement de même que le récepteur. De plus, la blockchain pourrait corriger l'un des risques de la hawala qui est celui du détournement de fonds par le hawaladar en se substituant à ces derniers.

---

[210] A.Y. SHEHU, . "The Asian Alternative remittance System and Money Laundering", 2003 in M.VALERI, R. FONDACARO, C. De ANGELIS et A. BARELLA, "The Use of Cryptocurrencies for Hawala in the Islamic Finance", *European Journal of Islamic Finance,* 11 octobre 2020.

[211] En juin 2016, l'agence Europol a fait savoir qu'une équipe commune composée d'enquêteurs belges, français et hollandais avait démantelé un blanchiment d'argent provenant d'un trafic de stupéfiants opéré entre le Maroc et l'Europe de l'Est et utilisant entre autre le système de la hawala pour blanchir les fonds

[212] *Après les attentats du 11 septembre 2001, les hawalas ont fait l'objet de l'attention des enquêteurs pour avoir pu être utilisés pour financer le terrorisme. En novembre 2001, l'administration Bush des États-Unis a fait geler les avoirs d'Al Barakat, une compagnie de paiement hawala somalienne très utilisée par la diaspora somalienne, et plusieurs agents de ce réseau ont été arrêtés*, , "Hawala", *Wikipédia*

[213] I. MAHAMOUD, « Comprendre le fonctionnement des hawalas : pour une meilleure régulation », *Techniques Financières et Développement*, 2014/1 (N° 114), p. 49-54.

B. La confiance dans la blockchain comme substitut à la hawala

117. - La confiance en la technologie blockchain pourrait remplacer la confiance dans un tiers intermédiaire. L'idée ontologique de la blockchain est en effet de reposer sur la confiance et la relation pairs-à-pairs. Elle tend à s'affranchir de tout intermédiation institutionnelle ou humaine pour mettre en relation des individus partageant une même idéologie libérale et anti étatique[214]. Cette idéologie peut - sans être analogue - se rapprocher de celle des terroristes fondée sur l'islamisme radical et la restauration du Califat par le djihad. Aussi, il n'est pas exclu que cette technologie réponde aux caractéristiques de la hawala.

118. - Des similitudes entre blockchain et hawala. En ce qu'elle met en relation au moins deux personnes quelle que soit leur situation géographique, la blockchain peut trouver à s'appliquer entre les groupes terroristes et leurs impétrants étrangers, à l'instar du système hawala. Par son caractère décentralisé, elle répond également à l'exigence de pallier l'absence d'institution bancaire. L'anonymat est également au cœur de ces deux mécanismes, même s'il ne repose pas sur un processus analogue : présence d'un tiers pour la hawala et recours à une adresse a-nominative dans la blockchain. La validation de la transaction par des membres de la blockchain peut être assimilée à la délivrance finale des fonds par l'intermédiaire après avoir apprécié l'identité réelle du bénéficiaire. Enfin, ces deux systèmes ont pour point de convergence de pouvoir poursuivre des fins licites ou illicites.

119. - Les spécificités de la blockchain permettent cependant de transcender la conception classique de la hawala. En se passant de tout intermédiaire, la blockchain permet de porter la confiance à son paroxysme. La notion de "Code is law[215]" parfois utilisée pour signifier la force des technologies numériques pour supplanter les modes classiques de régulation des sociétés, trouve ici une consécration. La constitution et la gestion d'une blockchain privée par des groupes terroristes[216] permettraient en effet de répondre aux exigences que satisfaisait la hawala tout en améliorant la sécurité des échanges. Dans cette figure, les paiements se feraient directement entre les membres de cette blockchain, préalablement identifiés. Le risque de détournement serait en théorie impossible dès lors que cette transaction devrait être validée par les autres membres de la blockchain et non par

[214] Voir à ce propos les développements sur la justification et la genèse de la technologie blockchain au n° 6.1.
[215] L.LESSIG, Code is Law – On Liberty in Cyberspace, Harvard Magazine, janvier 2000
[216] Il s'agit ici d'une hypothèse de travail qui n'apparaît en l'état pas susceptible de se réaliser. Toutefois, l'amélioration de la technicité de ses organisations et la réduction des coûts d'accès aux technologies pourraient à terme aboutir à une concrétisation de situation aujourd'hui dystopique.

un tiers isolé. Enfin, l'anonymat serait quasiment total en ce qu'aucun contact avec un tiers ne serait exigé. Il s'agit d'un exemple typique d'utilisation de la finance décentralisée - ou DéFI pour *Decentralized Finance*[217]. Ainsi selon le chercheur à l'IRIS Eric VERNIER : *"Les financements peuvent évidemment se faire beaucoup plus facilement via d'autres circuits. Il peut par exemple être plus simple de donner 1 000 euros directement à un imam radicalisé qui sert de relais local. Cependant, pour les moins de 30 ans qui touchent un peu en informatique, il est assez simple de passer par la cryptomonnaie. Et il lui paraîtra logique de passer par ce système plutôt que par un circuit traditionnel*[218]*".* L'attrait suscité par la crypto-monnaie peut donc également contribuer à sa diffusion parmi les terroristes les plus jeunes[219].

Section 2. L'émergence de modalités inhérentes à la technologie blockchain

120. - Solution de continuité, la blockchain est une technologie de rupture. Elle apporte dans son sillage un ensemble de dispositifs inédits et, par conséquent, inconnus. Or, le temps de la technique n'étant pas celui de la norme, un décalage chronologique et technologique se crée entre organisations criminelles et autorités étatiques. La criminalité sait exploiter les failles de la répression et s'approprier les nouvelles formes de commission des infractions. En tant que groupe, les terroristes sont représentatifs d'une forme particulière de criminalité organisée. Ils ont donc les moyens d'utiliser les modalités innovantes de criminalité, notamment dans le cadre de leur financement (**Paragraphe 1**).

La réaction des autorités étatiques est bien souvent latente et lacunaire. Elle semble ainsi reposer sur la dialectique Prométhée - Épiméthée[220]. La réponse étatique doit en effet, avant de pouvoir répondre efficacement à un risque, l'identifier et l'analyser. Or, dans le cas du financement du

[217] La finance décentralisée correspond au système financier parallèle et autonome par lequel les ses utilisateurs s'affranchissent du système bancaire formel et traditionnel. Il repose sur l'utilisation de la blockchain, des crypto-monnaies, voire des smart contracts pour créer un écosystème dans lequel les transactions se feront sans passer par un intermédiaire. Il repose donc sur le principe de peer-to-peer et peut par conséquent échapper à tout contrôle extérieur.

[218] , "Les cryptomonnaies, nouvelle arme des groupes terroristes ?", *France24*, 22 août 2019, consulté le 12 décembre 2022.

[219] Par exemple, le 31 janvier 2023, le procureur de Manhattan a annoncé la mise en accusation de Victoria JACOBS, une Américaine de 43, devant la Cour suprême de New-York des chefs de complicité d'acte de terrorisme par financenement. Elle aurait en effet envoyé près de 5000 dollars en crypto-monnaies au groupe "Malhama Tactical," un organisme terroriste basé en Syrie et destiné à la préparation militaire des recrues.

[220] Prométhée signifie celui qui réfléchit avant alors que Épiméthée désigne celui qui réfléchit après

terrorisme, les aspects occultes qui sont les siens rendent cette réponse sous dimensionnée (**Paragraphe 2**).

Paragraphe 1. Des modalités innovantes de financement du terrorisme

121. - Nombreuses sont les applications de cette technologie. Mais plus rares sont celles qui possèdent en germe des virtualités de financement du terrorisme nouvelles. Les jetons non fongibles - ou NFT - font partie de ces dispositifs qui génèrent en eux-mêmes une économie parallèle et autonome. Ils sont dès lors les vecteurs d'un terrorisme multidimensionnel, se caractérisant par l'apologie et la propagande, le recrutement ou encore le financement (A). Au-delà du monde réel, Le Métavers, en raison de sa transcendance et de sa difficile appréhension par les non-initiés, suscite également des craintes quant à une utilisation par les groupes terroristes (B).

A. Financer le terrorisme par les NFT

122. - Crowdfunding et financement du terrorisme. Les financements participatifs ont été imaginés pour soutenir financièrement des projets sociétaux ambitieux mais dépourvus du soutien public. Ils se sont développés dans tous les secteurs tels que l'environnement, l'immobilier ou l'aide humanitaire. Fondé sur un esprit philanthropique, le crowdfunding repose sur une accumulation de micro-financements et pouvant provenir de plusieurs pays. Les donateurs poursuivent en général une même finalité et partagent l'objet de leur soutien. Cependant, ce mécénat décentralisé peut être employé à des fins illicites, voire criminelles. Le développement des réseaux sociaux à accru la portée de ces appels aux dons ciblés et l'ancrage du Darknet dans la praxis de certains internautes a permis la naissance de financements dissimulés. Le terrorisme s'est emparé de ce vecteur[221]. Au regard des sommes parfois vénielles en jeu, *"l'objectif pour les pouvoirs publics est moins de tenter d'entraver ce type de financement que de les identifier pour retracer une véritable cartographie des flux financiers entre personnes impliquées dans les filières syriennes ou dans des actes de terrorisme[222]".* Cette cartographie pourrait être d'autant plus difficile à établir que les financements se feront par le recours aux NFT.

[221] Déjà dans son rapport de 2015 *Financing of the terrorist organisation Islamic State in Iraq and the Levant,* Le GAFI relevait que l'État islamique, par le biais de son compte officiel Al-Itisam , générait des "tempêtes de tweets" et attirait des financements en nombre via les réseaux sociaux. Le groupe islamiste obtenait alors des fonds par le biais de cartes prépayées après une prise de contact par Skype.

[222] Rapport n° 388 (2014-2015) de M. Jean-Pierre SUEUR, fait au nom de la CE moyens de la lutte contre les réseaux djihadistes, déposé le 1er avril 2015

123. - Usage des NFT dans le micro-financement participatif. Les jetons non fongibles sont générés par des smart contracts reposant eux-mêmes sur la blockchain. Créés ex-nihilo, ils peuvent contenir plusieurs informations différentes jusqu'à représenter une image existante telle qu'une œuvre. Les i*nitial coin offering* - ICOs - ou offres au public de jetons sont une illustration de la possibilité de mettre en place un appel aux dons par le biais des NFT. Il s'agit d'une "*opération de levée de fonds effectuée à travers un dispositif d'enregistrement électronique partagé, une blockchain qui donne lieu à l'émission de jetons servant, selon les cas, à obtenir des produits, des services ou des droits de la société émettrice*[223]*".* Les jetons sont payés en crypto-monnaies - bitcoin ou ethereum en général - et transitent par la blockchain, assurant ainsi l'anonymat de l'acheteur et du vendeur. Dès lors, cette nouvelle forme de levée de fonds suscite la méfiance des institutions de lutte contre le blanchiment de capitaux et de financement du terrorisme en raison de son détournement possible à des fins criminelles. Ces ICOs pourraient être le fait des organisations terroristes elles-mêmes mais plus certainement la résultante d'initiatives personnelles de la part de leurs sympathisants. Ainsi, un article du Wall Street Journal du 6 septembre 2022 faisait état de la découverte d'un jeton intitulé *IS-NEWS #01* et faisant l'éloge des combattants terroristes. Bien qu'il soit isolé, ce jeton - auquel deux autres ont succédé - souligne la nécessité de s'intéresser à ces nouvelles formes de financement pour en réguler le commerce, notamment par le biais de normes déclaratives renforcées à l'égard des émetteurs[224].

Toutefois, si le financement du terrorisme par les NFT se conçoit dans le monde réel, il peut également être dématérialisé et s'opérer par le recours au monde virtuel que représente le Métavers.

B. La dématérialisation du financement du terrorisme dans le Métavers

124. - Le Métavers a cette particularité de pouvoir recréer un environnement réaliste dans un univers virtuel. Il offre en effet tous les services qui sont par ailleurs présents à l'extérieur. Les utilisateurs peuvent ainsi commercer, investir dans l'immobilier, participer à des événements festifs ou encore y organiser des rassemblements. Il s'agit donc d'un monde parallèle, permanent et transcendant. Partant, comme dans le monde réel, la finance et plus généralement l'économie de marché, sont cardinaux dans le Métavers. À cet égard, ses thuriféraires ont développé de véritables

[223] TRACFIN, *Activités et analyses,* 2021 p. 95.
[224] Voir la partie II relative aux dispositifs répressifs.

superstructures financières, calquées sur les institutions financières traditionnelles, mais dotées de spécificités attrayantes pour les individus honnêtes comme malveillants.

125.- Les DAO dans le Métavers. Les DAO ou *Decentralized Autonomous Organisation* sont, à l'image *du crowdfunding dans le monde réel, des organismes de financement sont créés sans être des établissements de crédit traditionnels. Ils fonctionnent plutôt comme une communauté de personnes (ou d'avatars) qui s'organise elle-même*[225]*"*. Les DAO sont donc constituées par des groupes d'individus organisés et disposant de règles de fonctionnement inscrites dans la blockchain. Elles furent pensées pour financer des projets au sein de cette blockchain mais leur utilisation peut dépasser son seul cadre. Les DAO sont intéressantes par leur caractère décentralisé et autonome. Une fois les directives de fonctionnement enregistrées dans un bloc - comme par exemple les conditions d'acquisition d'un NFT - elles sont intangibles. Cela permet notamment de susciter des investissements dans des actifs numériques présents dans le Métavers au sein de ces DAO, sans immixtion de l'extérieur et le tout parmi une communauté d'individus partageant les mêmes motivations. En cela, la combinaison des DAO et du Métavers offre un support potentiel de financement du terrorisme. La première en permettant des financements participatifs entre membres d'un même groupe, le second en étant le support de ces investissements - qu'il s'agisse de NFT, de biens immobiliers ou encore de crypto-monnaies.

126. - Le Métavers est en lui-même une zone sombre de nature à être instrumentalisée par les groupes terroristes aux fins de commettre leurs exactions, mais également de financer leurs opérations. La possibilité pour les utilisateurs de cet univers d'y accéder de n'importe quel endroit du globe et d'y apparaître sous les atours d'un avatar au pseudonyme banal, risque d'être exploitée par les terroristes pour organiser des rencontres et transactions sans éveiller le moindre soupçon. Il serait en effet impossible de savoir à quel individu appartient tel avatar et de quelle origine proviennent les crypto-actifs. Sans représenter à lui seul un nouveau mode de financement du terrorisme, le Métavers en constitue toutefois un support certain. Il incarne ainsi ce qui pourrait être qualifier d'un terrorisme 3.0 : les attentats seraient financés et conceptualisés dans le Métavers mais seraient commis dans le monde physique avec des victimes réelles.

[225] B. DOUCET et I. DE LAMINNE, "Métavers : enjeux, risques et opportunités d'une réalité en devenir", *Regional IT Wallonie-Bruxelle*, juin 2022..

Paragraphe 2. Une réponse étatique sous-dimensionnée

127. - Schématiquement, l'appréhension d'une infraction comme le financement du terrorisme se concrétise par une double dynamique. Dans un premier temps, les autorités étatiques chargées de la lutte contre le terrorisme - et plus généralement de la criminalité - tentent d'en prévenir l'aboutissement en mettant en oeuvre des mesures fondées sur le risque. Cette approche préventive qui est désormais assimilée s'agissant des modes classiques de financement souffre néanmoins d'apories dès lors que sont envisagées les méthodes reposant sur la blockchain (A). Nonobstant l'échec de la prévention de l'infraction, les auteurs doivent être poursuivis et éventuellement condamnés. Or, si la sanction du financement du terrorisme est prévue par les textes répressifs, son effectivité dans le cadre du terrorisme 3.0 soulève des enjeux pregnants (B).

A. La difficile prévention du financement 3.0 du terrorisme

128.- La prévention du financement du terrorisme est historiquement un enjeu majeur que les États ont désormais placé au centre de leurs dispositifs de lutte contre le terrorisme. Analyser les flux financiers pour tenter d'en identifier les bénéficiaires et le cas échéant les juguler, tel est l'objectif des premiers textes internationaux en matière de lutte contre le terrorisme. Dans ce corpus, la résolution du 28 septembre 2001[226], adoptée par le Conseil de sécurité de l'ONU, et relative à la lutte contre le terrorisme fonde la dynamique qui sera suivie par la suite face à ce fléau au niveau international. Ce volontarisme fut par la suite repris au niveau de l'Union européenne dans le cadre des directives dites anti-blanchiment[227] établissant des normes LCB-FT - lutte contre le blanchiment et financement du terrorisme. Le point cardinal de ces instruments est d'être fondés sur une approche par les risques. Désormais inscrites dans le Code monétaire et financier[228], ces dispositions européennes offrent un cadre structurant de prévention du financement du terrorisme.

[226] Résolution 1373 (2001).
[227] Cinq directives sont pour l'instant en vigueur, elles ont toutes été transposées par la France. La cinquième directive est celle du 30 mai 2018 et à été transposée en droit français par l'ordonnance du 12 février 2020 renforçant le dispositif de lutte contre le blanchiment de capitaux et le financement du terrorisme.
[228] Code. mon. fin., Titre VI : Obligations relatives à la lutte contre le blanchiment des capitaux, le financement des activités terroristes, les loteries, jeux et paris prohibés et l'évasion et la fraude fiscales (Articles L561-1 à L564-2)

Les opérateurs financiers et bancaires doivent, lorsqu'ils interagissent avec des entités ou des personnes dont ils ont des raisons de penser qu'ils sont à risque, se soumettre à une série d'obligations. Or, "*l'ensemble s'articule autour de deux grands axes, selon que les mouvements de capitaux transitent par des personnes qui en assurent occasionnellement le principe ou, au contraire, par des institutionnels ou professionnels agissant de façon habituelle*[229]*"*. Mais cette sujétion trouve une limite lorsque est mise en œuvre une transaction par la blockchain. Qu'il s'agisse des opérateurs occasionnels (1) ou professionnels (2), il semble difficile de pouvoir reproduire le schéma classique de détection des financements terroristes.

1. Le problème d'identification des opérateurs occasionnels recourant à des transactions en crypto-monnaies

129. - Aux termes de l'article L.561-1 du Code des marchés financiers : *"les personnes autres que celles mentionnées à l'article L. 561-2 qui, dans l'exercice de leur profession, réalisent, contrôlent ou conseillent des opérations entraînant des mouvements de capitaux, sont tenues de déclarer au procureur de la République les opérations dont elles ont connaissance et qui portent sur des sommes qu'elles savent provenir de l'une des infractions mentionnées à l'article L. 561-15"*. Ce texte soumet ainsi les entités ou individus qui se livrent de manière ponctuelle, voire isolée, à des opérations de transferts de capitaux à une obligation de déclaration au procureur de la République lorsqu'elles soupçonnent que les fonds proviennent d'une infraction ou qu'elles savent destinée au financement du terrorisme. Ce texte, qui se rapproche de l'article 40 du Code de procédure pénale[230], postule donc que l'opérateur soit identifié. Mais dans le cadre d'une transaction par la blockchain, l'usage d'une adresse anonyme par les utilisateurs rend presque impossible cette identification. Ainsi, il apparaît que cette obligation soit pour l'heure inapplicable à cette technologie, ce qui obère les chances de prévenir ce mode de financement qui, dans le cadre des terroristes isolés, est probablement le plus usité.

[229] Y. MAYAUD, "Terrorisme - Prévention", *Répertoire de droit pénal et de procédure pénale,* Dalloz, février 2020.

[230] C. pr. pén., art. 40 al.2 : "*Toute autorité constituée, tout officier public ou fonctionnaire qui, dans l'exercice de ses fonctions, acquiert la connaissance d'un crime ou d'un délit est tenu d'en donner avis sans délai au procureur de la République et de transmettre à ce magistrat tous les renseignements, procès-verbaux et actes qui y sont relatifs".*

2. L'assujettissement des PSAN, une avancée nécessaire mais insuffisante

130. - Les prestataires sur actifs numériques sont "*un dispositif ayant pour objet la régulation du marché lié aux devises numériques*[231]*"*. Plus précisément, il s'agit d'un prestataire de service qui accomplit à titre professionnel l'une des activités énumérées par le Code monétaire et financier dans sa version issue de la loi du 22 mai 2019 - dite loi Pacte. Dans sa volonté d'étendre le champ d'application des dispositions LCB-FT, la cinquième directive européenne a intégré ces PSAN dans la liste des professionnels assujettis[232]. Désormais, ces derniers doivent se soumettre aux obligations de vigilance et de déclarations de soupçons auprès de TRACFIN[233]- le service de renseignement financier du ministère de l'Économie et des Finances[234]. Mais bien que ce dispositif ait fait ses preuves dans son application aux professionnels assujettis initialement[235], son efficacité, voire son effectivité, semble compromise s'agissant des PSAN. En effet, le propre des transferts de fonds par le biais des crypto-monnaies est d'être volontairement décentralisés. Ainsi, bien que les PSAN offrent des services d'échanges ou d'envois d'actifs numériques, les groupes terroristes ne les utiliseront pas et continueront à profiter de l'anonymat et de la fluidité offertes par la blockchain. Il ne s'agit donc pas d'une problématique tenant à l'encadrement des acteurs de la blockchain - bien que cet encadrement soit nécessaire - mais de la blockchain elle-même. Par conséquent, il sera démontré lors des développements relatifs aux moyens d'adaptation de la lutte à la technologie blockchain que cette dernière doit et peut être encadrée.

B. La qualification incertaine du financement du terrorisme 3.0 du terrorisme

131. - Le financement du terrorisme est une infraction d'une particulière gravité exposant son auteur à des peines sévères. En effet, le rôle central du financement dans la préparation et la commission des attentats terroristes ayant émaillé les sociétés occidentales a fait de cette étape préalable au crime une cible première des sanctions nationales et internationales. Toutefois, dans leur conception classique, ces sanctions se révèlent inadaptées face au développement de la blockchain pour la réalisation de ces actes[236]. Mais avant de pouvoir condamner et sanctionner cette

[231]A.ROBINE, "Qu'est-ce qu'un PSAN ?" Captaincontrat.com, 2 novembre 2022, consulté le 10 décembre 2022.
[232] C.mon.fin., art. L. 561-2, 7° bis et 7 °quater.
[233] Ibid, L. 561-4-1 à L.561-14-2 et L.561-15 à L.561-22.
[234] Voir la partie II sur la lutte.
[235]Selon le ministère de l'Economie et des Finances : *"Le Groupe d'Action Financière (GAFI) a publié le 17 mai dernier son rapport d'évaluation du dispositif français de LBC-FT. Au terme de cette procédure qui s'est déroulée sur plus de deux ans, la France a obtenu d'excellents résultats et se place ainsi au premier rang des pays luttant efficacement contre la criminalité financière. Le rôle central joué TRACFIN et la qualité du renseignement financier y sont soulignés",* voir *Rapport d'évaluation mutuelle de la France 2022*
[236] Voir les développements relatifs aux enjeux d'adaptation de la répression des infractions commises par la blockchain.

infraction, il faut tout d'abord en établir les éléments constitutifs. Or, les circuits auxquels les crypto-monnaies donnent lieu peuvent rendre difficile une telle opération au regard du principe de légalité criminelle[237].

132. - L'élément matériel de l'infraction ne soulève a priori pas de problème de qualification. L'article 421-2-2 du Code pénal vise le fait de : *"financer une entreprise terroriste en fournissant, en réunissant ou en gérant des fonds, des valeurs ou des biens quelconque ou en donnant des conseils à cette fin"*. En raison de sa définition large, le financement du terrorisme semble pouvoir recouvrir les formes les plus innovantes de financement d'une entreprise terroriste, et notamment celles recourant aux crypto-actifs - considérés comme des biens meubles incorporels[238]par la doctrine et la jurisprudence. La seule incertitude pourrait se cristalliser autour de la notion de fourniture en ce que la transaction par la blockchain n'a pas lieu dès l'envoi des crypto-monnaies mais seulement lorsque l'opération est enregistrée par les nœuds de la chaîne de blocs. Or quelle sera la qualification de l'émission d'une crypto-monnaie à une entreprise terroriste dont la validation a été refusée par les mineurs ? Doit-elle être assimilée à une tentative ? L'existence d'un commencement d'exécution - l'émission du jeton - et l'absence de désistement volontaire - le refus des mineurs - devrait aboutir à une telle conclusion au regard de la combinaison des articles 421-5[239] et 121-5[240].

133.- L'élément moral du financement du terrorisme suscite plus de réserves. Le texte précise en effet que l'auteur doit avoir "*l'intention de voir ces fonds, valeurs ou biens utilisés ou en sachant qu'ils sont destinés à être utilisés, en tout ou partie, en vue de commettre l'un quelconque des actes de terrorisme[241] (...)"*. Pour être condamné, l'auteur de l'acte de fourniture, de réunion ou de gestion des valeurs destinées à financer le terrorisme doit vouloir ou à tout le moins avoir conscience d'inscrire son acte dans le cadre d'une entreprise terroriste. Or, le principe même de la blockchain est de ne pas permettre de connaître - sauf exception - l'identité des parties à la transaction. Par hypothèse, un individu pourrait acheter un NFT tout à fait banal - une oeuvre d'art, un bored

---

[237] C. pén., art. 111-3 : *"Nul ne peut être puni pour un crime ou pour un délit dont les éléments ne sont pas définis par la loi, ou pour une contravention dont les éléments ne sont pas définis par le règlement.*
Nul ne peut être puni d'une peine qui n'est pas prévue par la loi, si l'infraction est un crime ou un délit, ou par le règlement, si l'infraction est une contravention".

[238] A. CAPRIOLI, "La nature du Bitcoin enfin précisée", note ss T. com. Nanterre, 6e ch., 26 févr. 2020, n° 2018F00466 (non publié)

[239] C.pén., art. 421-5 al.2 : *"La tentative du délit défini à l'article 421-2-2 est punie des mêmes peines".*

[240] C.pén., art. 121-5 : *"La tentative est constituée dès lors que, manifestée par un commencement d'exécution, elle n'a été suspendue ou n'a manqué son effet qu'en raison de circonstances indépendantes de la volonté de son auteur".*

[241] C.pén., art. 422-2-2.

apes[242]ou un autre avatar, de manière purement spéculative. S'il n'est pas averti de ce que ce jeton sert en réalité à financer une opération à caractère terroriste, il ne peut pas se voir reprocher d'avoir voulu ou su qu'il y a contribué. L'élément moral ne saurait alors être caractérisé à son encontre. Dès lors, l'anonymat de la blockchain sera encore une fois un obstacle - non pas à l'identification par les autorités de poursuites des criminels - mais à la connaissance par le spéculateur de bonne foi de la nature de son investissement. Face à cette aporie de la qualification de l'élément moral, la jurisprudence de la Chambre criminelle pourrait faire oeuvre créatrice - comme elle en a le tropisme - afin d'établir une présomption de connaissance de l'entreprise terroriste[243] dès lors que l'achat ou l'investissement est entouré de circonstances au vu desquelles l'agent ne pouvait ignorer la nature de son acte.

Conclusion du Chapitre I

134.- Le financement du terrorisme est donc l'un des piliers auxquels il faut s'attaquer pour endiguer la menace que représente cette technologie. Utilisée très en amont de l'acte terroriste, elle n'en devient pas moins l'un de ses éléments constitutifs. Devenant une nouvelle forme de financement dont il est permis de penser qu'elle pourrait se renforcer en écho au déclin de la centralité des organisations terroristes, la blockchain fait naître des risques que la réponse actuelle des autorités étatiques a du mal à appréhender. Mais sans négliger la préparation de l'infraction, il faut aussi en limiter la dissimulation (**Chapitre II**).

[242] Ces avatars inscrits sur un jeton sont développés par Yuga Labs et prennent la forme de Singe sur la blockchain Ethereum notamment. Ils connaissent une spéculation massive et atteignent des prix très élevés.

[243] A cet égard, dans le sommaire de sa décision rendue le 7 septembre 2021 dans l'affaire Lafarge et relative à des faits de financement de l'État islamique par cette entreprise en Syrie, la Cour précise que "*doit être approuvée la chambre de l'instruction dont les énonciations, procédant de son appréciation souveraine des faits, font ressortir que la société mise en examen et sa filiale en Syrie ont versé, par des intermédiaires, plusieurs millions de dollars à l'organisation dénommée Etat islamique et à d'autres groupes terroristes afin de sécuriser l'acheminement des salariés employés localement, alors qu'il résultait de ses constatations que la société ne pouvait ignorer le caractère terroriste de cette organisation"* . L'impossible ignorance est donc déjà une clef de lecture utilisée par la Cour de cassation pour apprécier l'élément moral du financement du terrorisme.

Chapitre II. En aval : le blanchiment de capitaux par le système blockchain

135.- Dans la criminologie rationnelle, la faculté pour les criminels de pouvoir blanchir le produit de l'infraction est une motivation supplémentaire du passage à l'acte. Ainsi, *"le blanchiment d'argent correspond à un ensemble d'actes chronologiquement second, débutant par définition après la commission d'une première infraction pénale dont le produit financier, sale, doit être blanchi[244]".* Juridiquement, l'article 324-1 du Code pénal distingue deux formes de blanchiment. Est en effet réprimé : *"le fait de faciliter, par tout moyen, la justification mensongère de l'origine des biens ou des revenus de l'auteur d'un crime ou d'un délit ayant procuré à celui-ci un profit direct ou indirect"* ainsi que *"fait d'apporter un concours à une opération de placement, de dissimulation ou de conversion du produit direct ou indirect d'un crime ou d'un délit"*. Un auteur établit donc une dichotomie entre le blanchiment immédiat - portant sur le patrimoine criminel - et le blanchiment médiat - portant sur le patrimoine du criminel[245].

136.- Diversité d'actes pour finalité unique. Le blanchiment de capitaux est une infraction polymorphe dont la réalisation n'est limitée que par l'imagination des criminels. Dès lors, si sa finalité est unique - faire apparaître licite des fonds ou un patrimoine illicite - les méthodes employées sont variées. De plus, et pour cette même raison, l'infraction principale ayant procuré l'objet blanchi peut elle-même être très diverse. Cette hétérogénéité dans la praxis criminelle est une des sources principales de difficulté pour les enquêteurs. Les procédés de blanchiments sont souvent complexes et font intervenir des réseaux organisés et internationaux.

137.- Au regard de ses caractéristiques propres, la blockchain semble être un dispositif potentiel du blanchiment. Elle soulève en cela des enjeux nouveaux en matière de répression, tant s'agissant des modes de commission de l'infraction que des poursuites subséquentes. Comme toute technologie innovante, elle risque d'être utilisée par des groupes de criminalité organisée adeptes de ces leviers d'impunité. Elle pourra renouveler les procédés classiques de blanchiment en en

[244]A.AMICELLE, "La reconstruction par association des problèmes publics : retour sur l'invention du blanchiment d'argent", *Criminologie*, *49*(1), 2016, p. 25–50.
[245] M. SEGONDS, "Les métamorphoses de l'infraction de blanchiment... ou les enjeux probatoires de la lutte contre le blanchiment*" AJ Pénal 2016 n°4*, p. 168.

permettant la mise en œuvre. À cet égard, les crypto-monnaies pourraient jouer un rôle central pour faciliter le blanchiment d'argent (**Section 1**).

De surcroît, les possibilités offertes par la technologie blockchain sont susceptibles de créer de nouvelles formes de blanchiment, nécessairement imprévisibles et jouant sur les fonctions de cet instrument. Ces nouveaux schémas de blanchiment permis par la blockchain sont donc une menace de plus dans le cadre de la lutte contre ce phénomène (**Section 2**).

Section 1. Le blanchiment d'argent facilité par les cryptos monnaies

138. - Blanchir pour obscurcir, un oxymore criminel. Comme son nom ne l'indique pas, le blanchiment de capitaux est une infraction qui tend à masquer l'origine ou la destination de fonds illicites. En effet, cette "infraction de résultat[246]" consiste dans "*le fait de dissimuler ou de déguiser le mouvement de biens dont celui qui s'y livre sait qu'ils proviennent d'une activité criminelle*[247] *"*. Aussi, pour aboutir à un tel résultat, les criminels - agissant généralement dans le cadre de structures organisées - cherchent les moyens de faire disparaître la genèse de cet enrichissement. Le triptyque placement - dissimulation - conversion[248]est le paradigme de cette entreprise. Dans ce contexte, la blockchain offre des possibilités concrètes en raison de ce qui en fait l'identité.

139. - L'anonymat conféré par cette technologie de la chaîne de blocs est prôné par ses adhérents et redouté par ses détracteurs. Il résulte à la fois de son processus de fonctionnement et plus profondément de son idéologie. Il donne à son utilisation un aspect mystérieux - pour ne pas dire mystique - ce qui renforce les antagonismes y relatifs. L'anonymat est fortement soluble dans la commission des infractions et leur dissimulation. Il fait naître une criminalité volatile et insaisissable. Par conséquent, la force de l'anonymat offert par la blockchain devra être interrogée au regard de ses effets en matière de blanchiment de capitaux (**Paragraphe 1).**

140.- La complexité d'appréhension du phénomène de blanchiment est qu'il se conçoit indépendamment de toutes frontières territoriales. Les groupes organisés de criminels sont devenus des multinationales agissant depuis l'étranger par le biais de leurs filiales. Dès lors, il est

[246] N. CATELAN, "Les avatars : recel, blanchiment et NJR", *Droit pénal des affaires,* 30 mars 2021.
[247] Cass. Crim. 18 mars 2020, n° 18-86.491
[248] Op. cit., N. CATELAN.

permis de se demander si l'a-territorialité de la blockchain pourrait exacerber cette dynamique et par la même en accroître le développement (**Paragraphe 2**).

Paragraphe 1. La force de l'anonymat offert par la blockchain

141. - S'interroger sur la force de l'anonymat permis par la blockchain signifie que ce dernier n'est pas absolu. Mais bien que relative, cette opacification de l'identité est une tentation bien trop grande pour n'être pas investie par les groupes désireux de blanchir leurs capitaux. En effet, il est suffisamment fort pour rendre les opérations de blanchiment complexes à déceler. Ainsi, malgré la relativité de cet anonymat, sa dangerosité devra être précisée (A). D'autant plus que ce pseudonymat[249] n'est pas condamné à n'être qu'une interface franchissable. Il peut, par différents moyens informatiques, être renforcé et se rapprocher d'un quasi-anonymat (B).

A. Un anonymat relatif mais suffisant

142. - Rappels sur le fonctionnement de la blockchain. L'exécution d'une transaction suppose la création d'une clef publique, laquelle correspond à l'adresse publique sous laquelle les transactions seront enregistrées et consultables dans la blockchain publique. Or, cette adresse publique correspond à une suite de chiffres et de lettres propres au portefeuille de l'utilisateur. Elle s'apparente en cela au RIB d'un compte bancaire.

143. - Bien que n'étant pas intraçable, cette adresse est un puissant vecteur de blanchiment de capitaux. En effet, en permettant aux groupes criminels d'utiliser des identités d'emprunt, elle se substitue à la création d'une structure licite telle qu'un compte bancaire, par lequel les flux "d'argent sales" seraient envoyés afin d'être convertis et réinjectés dans l'économie légale. Toute la problématique de cette infraction est en effet de donner une apparence de légitimité à une opération économique criminelle. Or, l'accumulation de mouvements de fonds entre plusieurs comptes est de nature à éveiller les soupçons des banques, d'une part, et des autorités de contrôle étatiques, d'autre part. Aussi, pour pallier ce risque, le recours à des opérations de transferts de capitaux par le biais de la technologie blockchain est envisageable et même redoutable. Le schéma serait similaire à celui utilisant jusqu'alors les services bancaires : la création d'une adresse de crypto-monnaie -

[249] Néologisme désignant la dissimulation de l'identité d'un individu recourant à un pseudonyme.

comme le bitcoin - ; l'envoi de fonds d'origine illicite à cette adresse depuis une autre adresse, elle-même sous pseudonyme ; in fine, la conversion de ces bitcoins en d'autres crypto-monnaies ou leur réinjection dans l'économie réelle.

144.- Les risques induits par cet anonymat relatif sont considérés à long terme comme élevés par le Conseil d'orientation et de lutte contre le blanchiment[250]. En effet, la difficile identification des entités qui opèrent sur le système blockchain constitue un obstacle à la répression du blanchiment. Mais plus encore, la mise en oeuvre des dispositifs de prévention du blanchiment - fondés sur la connaissance des bénéficiaires effectifs[251]- est par nature compromise dans ce contexte. Il est alors indispensable de renforcer cette prévention en l'adaptant à cette nouvelle forme de criminalité.

B. Un pseudonymat renforcé par la cryptologie

145. - La cryptologie est à la fois la technologie sous-jacente de la blockchain mais également un moyen de renforcer son caractère anonyme. Il existe en effet des crypto-monnaies à anonymat renforcé qui sont par conséquent privilégiées dans le cadre d'opérations illicites. A titre d'exemple, la crypto-monnaie Monero est l'une des plus usitées sur le Darknet et par les organisations criminelles[252]. Son fonctionnement est fondé sur la cryptographie déclinée sous plusieurs aspects[253].

146.. - Les adresses utilisées pour les transactions Monero sont créées aléatoirement par un algorithme plus performant que celui du Bitcoin. Ces dernières sont ainsi uniques et confidentielles. Par ailleurs, chaque transaction doit être effectuée par une adresse différente. Cette exigence rend

---

[250] "Analyse nationale des risques de blanchiment de capitaux et de financement du terrorisme en France", *Rapport du Conseil d'orientation de la lutte contre le blanchiment decapitaux et le financement du terrorisme,* septembre 2019.

[251] C. mon. fin., art. L. 561-5, I : "*Avant d'entrer en relation d'affaires avec leur client ou de l'assister dans la préparation ou la réalisation d'une transaction, les personnes mentionnées à l'article L. 561-2*
1° Identifient leur client et, le cas échéant, le bénéficiaire effectif au sens de l'article L. 561-2-2 (...)
Ibid, art. R. 561-5 : *"Pour l'application du 1° du I de l'article L. 561-5, les personnes mentionnées à l'article L. 561-2 identifient leur client dans les conditions suivantes :*
1° Lorsque le client est une personne physique, par le recueil de ses nom et prénoms, ainsi que de ses date et lieu de naissance ;
2° Lorsque le client est une personne morale, par le recueil de sa forme juridique, de sa dénomination, de son numéro d'immatriculation, ainsi que de l'adresse de son siège social et celle du lieu de direction effective de l'activité, si celle-ci est différente de l'adresse du siège social (...)"

[252] Ainsi, certains hackers demandent le paiement de la rançon, dans le cadre d'un rançongiciel, uniquement en Monero. D'autres garantissent même une diminution de cette rançon en cas d'adoption de cette crypto-monnaie in "Monero, tout savoir sur la monnaie préférée du Dark Web", Le Big Data.fr, 21 janvier 2022.

[253] Ibid.

donc impossible le traçage de l'auteur commun des transactions comme ce peut être le cas avec les autres crypto-monnaies.

147.- La signature par cercles permet de mélanger l'adresse de l'expéditeur avec l'adresse d'autres individus. Ce faisant, elle crée un ensemble d'adresse expéditrice au sein duquel il n'est pas possible d'identifier celle qui est à l'origine de l'émission. Ainsi, l'individu se fond dans la masse des autres utilisateurs de cette crypto-monnaie et disparaît.

148.- Ces deux caractéristiques de Monero sont par nature criminogènes. En rendant impossible l'identification des utilisateurs, elles sont une garantie d'impunité pour les auteurs d'infraction et leur blanchiment. Là où il était possible de retracer l'origine d'une transaction en bitcoins, la neutralisation de tout lien entre l'émetteur et le bénéficiaire efface subséquemment le suivi des transferts jusqu'au criminel.

150.. - La rapidité de Monero, enfin, est un gage d'efficacité de cette crypto-monnaie. La durée de validation est d'environ cent-vingt secondes par transaction contre dix minutes pour un bitcoin[254]. L'accélération des échanges est toutefois problématique dans le cas d'une utilisation dévoyée de la blockchain, notamment pour le blanchiment de capitaux. Elle rend encore plus difficile le contrôle des flux ce qui accroît ainsi le profit généré par ces criminels à l'insu des autorités de contrôle.

Paragraphe 2. L'a - territorialité de la blockchain[255]

151.- La territorialité exprime, *"outre un contenu juridique d'appropriation, un sentiment d'appartenance, mais aussi d'exclusion, et un mode de comportement au sein d'une entité, qu'elle qu'en soit l'étendue, quel que soit le groupe social qui le gère[256]"*. L'idée que sous-tend la notion de territorialité est donc celle d'un lien entre une activité et un territoire donné. Elle signifie que les comportements individuels ou collectifs sont nécessairement pensés et accomplis dans ce cadre. Traditionnellement, le principe de territorialité est appréhendé dans une dimension étatique : c'est au sein des États que sont observés la plupart des phénomènes sociaux.

[254] "Comparatif des crypto-monnaies, IG.com.
[255] Titre inspiré de l'article J. GOLDSZLAGIER – A. LE TEURNIER, "La lutte contre le blanchiment à l'épreuve de la territorialité des crypto-actifs", AJ Pénal, 2021, 465.
[256] Glossaire Géoconfluence, *Territoire, Territorialisation, Territorialité,* ENS Lyon, juin 2022 disponible sur le site http://geoconfluences.ens-lyon.fr/glossaire/territoires-territorialisation-territorialite.

152.- Par négation, l'a-territorialité consiste en l'absence d'identité nécessaire entre un comportement et un État. Elle est la fille de la mondialisation et de l'internationalisation des échanges économiques et humains contemporains. Tous les faits sociaux sont concernés et notamment la criminalité. Or, la blockchain semble répondre à un double mouvement de décentralisation et de déterritorialisation.

153. - La décentralisation de la blockchain, liée à sa conception originelle[257], la rend très sensible aux comportements déviants, voire criminels. Elle permet à des groupes suffisamment puissants de prendre le contrôle de cette technologie et de commettre par là-même des infractions. Aussi, il convient de préciser comment ce caractère inhérent à la blockchain peut être exploité dans le cadre du blanchiment de capitaux (A).

154. - La déterritorialisation - entendue ici comme l'affranchissement des frontières établies par le recours à des moyens de communication toujours plus performants, c'est-à-dire, comme un *"affaiblissement des contrôles d'accessibilité et donc de contrainte spatiale imposées par les États"* - soulève également des problématiques sécuritaires [258]. Elle complexifie des schémas de blanchiment déjà difficiles à saisir. Elle permet aussi de mettre à profit les failles de systèmes juridiques étrangers dépourvus d'une législation suffisante, voire complaisants à l'égard des criminels. Là encore, la technologie de la chaîne de blocs offre un exemple de ces nouvelles techniques de communications affranchies des frontières. Partant, cette absence de lieu de commission de l'infraction - laquelle peut être commise depuis et vers tout endroit du globe - fait sourdre des enjeux renouvelés par l'utilisation de la blockchain (B).

[257] La blockchain a été pensée pour s'affranchir des pouvoirs publics, particulièrement dans le domaine économique, à la suite de crises successives comme celle de 2008, comme le rappelle L.SANTOLINI, *La stabilité économique, sociale et politique à l'ère du numérique : Exploration des options qui s'offrent aux régulateurs en matière de réglementation des crypto-monnaies,* Louvain School of Management, Université catholique de Louvain, 2019

[258] B. BADIE, *La Fin des territoires*, Fayard, 1995 in Glossaire Géoconfluence, *Territoire, Territorialisation, Territorialité* préc.

A. La décentralisation comme vecteur de blanchiment

155. - Le schéma classique d'une opération de blanchiment se décompose en un triptyque. Est en effet généralement observée l'existence d'un placement, d'un empilage et d'une intégration[259]. Le placement consiste à *"transformer des sommes d'argents en espèces provenant d'une infraction en un autre instrument financier monétaire ou en un autre bien[260]"*. Dans cette situation, la blockchain pourra intervenir en sa qualité de support de transactions en crypto-monnaies[261]. L'empilage désigne le fait de *"brouiller les pistes de l'origine des fonds par la multiplication des opérations bancaires ou financières successives faisant intervenir divers comptes, établissements, personnes, produits et pays[262]"*. Dans cette étape, il sera notamment question de l'utilisation de la blockchain aux fins de faciliter les transferts de capitaux de manière décentralisée, sans contrôle étatique ou privé. Pour cela, les organisations criminelles pourraient exploiter leur force d'influence afin de créer un "éco-système de blanchiment". Enfin, *"l'intégration vise à investir les fonds d'origine frauduleuse dans les circuits légaux de l'économie et en tirer des bénéfices"*[263]. Il s'agit ici de l'étape finale du blanchiment permettant à ces auteurs de profiter de fonds devenus licites. À cet égard, la blockchain constitue une source nouvelle dont les déclinaisons devront être explorées à l'aune des nouveaux dispositifs de blanchiment qu'elle apporte.

156.- L'empilage facilité par la décentralisation. Pour confondre les flux d'argent et ainsi en effacer les sources, les techniques usitées par les criminels varient. Ces derniers, composant avec leur époque, assimilent les nouveaux vecteurs de transfert de capitaux afin d'en maîtriser la logique et de les instrumentaliser. La blockchain fait partie de ces vecteurs et sa maîtrise est donc nécessaire pour ces agents.

157.- De l'usage des attaques 51 % ou Sybil, il est permis de craindre une prise de possession de la blockchain par les groupes les plus développés et ce dans le but de blanchir des capitaux. En effet, dès lors qu'ils seraient maîtres des transactions, ils pourraient les multiplier à l'envi, sans intermédiaire et ce avec une célérité inégalée. Par ce monopole, il serait impossible d'empêcher les

[259] Voir notamment A. LEPAGE, P. MAISTRE DU CHAMBON, R. SALOMON, Droit pénal des affaires, 5 e édition, p.163.
[260] Ibid.
[261] Voir dans ce chapitre la section relative aux nouveaux schémas de blanchiments permis par la blockchain.
[262] Op. cit, N. CATELAN, *Droit pénal des affaires*.
[263] Ibid.

fonds - préalablement transformés en crypto-monnaies - de transiter d'un portefeuille à l'autre et de brouiller leur origine. Il ne s'agit ici rien moins que d'une modernisation des techniques classiques de blanchiment par envoi d'argent sur des comptes situés à l'étranger[264]. La différence est toutefois fondamentale dans cette configuration en ce que le contrôle de ces flux est rendu excessivement complexe par les caractéristiques déjà présentées de la blockchain. Bien qu'étant en pratique difficilement concevable[265], ce risque est néanmoins présent et nécessairement croissant[266].

B. L'absence d'implantation territoriale au service du blanchiment

159.- Ce qui rend la poursuite du blanchiment éminemment complexe est sa dimension internationale. La commission de cette infraction résulte bien souvent d'une succession d'opérations réalisées dans différents pays, voire continents. Or, la blockchain est par nature dépourvue de toute implantation étatique. Il s'agit même d'une technologie mondiale en ce que le réseau est accessible à tous, quelle que soit leur localisation, à condition qu'ils disposent d'un moyen informatique pour s'y connecter. Plus précisément, cette a-territorialité de la blockchain se conçoit à deux niveaux : au niveau national par l'absence d'entité établie et identifiable ; au niveau international par l'absence de lien de rattachement avec un pays en particulier.

160.- Le fait que la blockchain ne soit pas incarnée dans une structure locale constitue à la fois une opportunité pour les organisations criminelles et en contrepoint une faiblesse pour les autorités étatiques. Comment contrôler les opérations de transfert d'argent sans pouvoir identifier la personne - physique ou morale - qui fait office d'intermédiaire ? En effet, si "*l'on ne peut attribuer à un support physique unique, susceptible d'autoriser un critère de rattachement physique ou juridique pertinent, les informations relatives à un actif numérique*[267]*",* il sera impossible d'en suivre les mouvements. Aussi, *"elle constitue en retour un défi considérable pour l'État dans l'exercice de ses prérogatives souveraines, telles que la défense de l'ordre public*[268]*"*. Dès lors, pour pallier cette

[264] Voir notamment, Cass. Crim, 14 janvier 2009, pourvoi n° 08-82.095
[265] En raison de la puissance nécessaire pour prendre le contrôle d'une blockchain de grande ampleur.
[266] Selon le *Guardian*, *"Un consortium de minage «Ghash.io» est parvenu à détenir 51% de la puissance de calcul de la blockchain Bitcoin ce qui leur donnait la faculté d'effectuer une transaction fictive sur la blockchain, de la faire valider à l'aide de ses propres «miners» détenant la majorité de la puissance de calcul, et de l'inscrire sur la chaîne de blocs",* in P. DE PREUX et D. TRAVILOVIC, "Blockchain et lutte contre le blanchiment d'argent, Le nouveau paradoxe ?", Expert Focus, 1er février 2018.
[267] J. GOLDSZLAGIER – A. LE TEURNIER, La lutte contre le blanchiment à l'épreuve de la territorialité des crypto-actifs, AJ Pénal, 2021, 465
[268] Ibid.

limite de la surveillance, il conviendra d'agir sur la technique elle-même - c'est-à-dire la blockchain[269] - et non sur les acteurs qui, par définition, ne seront pas coopératifs.

161. - Le risque de forum shopping. Ce concept désigne le "*choix d'une juridiction en raison des avantages, de procédure ou de fond, qu'on en attend*[270]". Il répond donc à une rationalité des individus choisissant de se placer sous l'empire de la législation la plus favorable. Or, comme il le sera démontré plus loin[271], l'approche de la blockchain par les États diffère grandement et son encadrement n'est pas homogène. Ainsi, il existe des zones de non droit au sein desquelles les obligations relatives - notamment à la lutte contre le blanchiment - ne s'appliquent pas ou peu. En raison de sa décorrelation d'avec une réalité territoriale, la blockchain est donc un moyen pour les criminels d'agir depuis et contre des pays tolérants ou impuissants. Couplé à son absence de dimension physique, elle est donc l'arme idéale pour la commission de nouvelles formes de blanchiment.

Section 2. De nouveaux schémas de blanchiment permis par la blockchain

163.- Les actifs numériques risquent de donner un nouveau visage aux opérations de blanchiment. Les crypto-monnaies sont à ce titre des instruments intéressants pour améliorer les différentes étapes de placement, d'empilage et d'intégration. S'agissant du placement, l'anonymat qui les entoure les rend attractifs afin d'investir de manière discrète, voire occulte, dans des entreprises parfois illicites. Dans le cadre de l'intégration, la variabilité de leur usage et leur fongibilité en font des instruments probables aux fins de diffusion dans l'économie réelle. Ces deux étapes, bien que distinctes, ont en commun de reposer sur la relation entre les actifs numériques et la monnaie légale dans le cadre de blanchiment dit "crypto-to-fiat" (**Paragraphe 1**).

Dans le cadre de l'empilage - parfois appelé conversion - ces actifs permettent une multiplication des échanges. De plus, des dispositifs ont été imaginés pour renforcer l'anonymat de leurs utilisateurs ce qui contribue à rendre d'autant plus opaque ce mode de blanchiment dit "crypto-to-crypto" (**Paragraphe 2**).

[269] Voir le titre II de la seconde partie et notamment le chapitre consacré à la modernisation des techniques d'enquête.
[270] FranceTerme, ministère de la Culture.
[271] Voir dans la partie II le chapitre 2 du titre I relatif à la coopération internationale.

Paragraphe 1. Le blanchiment « crypto to fiat »

164.- L'expression "crypto-to-fiat" désigne la conversion de crypto-monnaies en monnaies dites "fiat", c'est-à-dire, *"la représentation monétaire mise en place par un État, sous gestion d'une banque centrale*[272]*"*. Il s'agit donc de l'unité de valeur qui est unanimement admise au sein d'un État ou d'une institution d'État aux fins de réaliser des transactions marchandes. Cette distinction permet de saisir l'ambivalence des crypto-actifs qui, bien qu'étant revêtus d'une valeur économique certaines, ne sont pas pour autant des monnaies légales produites par l'État[273]. Cette dichotomie est au cœur du blanchiment de capitaux.

165.- Des "monnaies fiats" aux crypto-actifs. Passer d'une monnaie légale à un actif numérique peut offrir des avantages aux criminels désireux de dissimuler l'origine illicite de ces fonds. En effet, les qualités présentées des crypto-monnaies en font des instruments topiques de blanchiment par placement en ce qu'ils affaiblissent le lien entre l'argent et le crime. Pour ce faire, l'attractivité économique des actifs numériques constitue une motivation pour en faire des sources d'investissement exotiques (A)

166. - A l'inverse, le passage des crypto-actifs aux monnaies légales semble subordonné à des considérations d'ordre socio-économique sources d'incertitudes. La volatilité avérée de la plupart de ces actifs éloigne d'autant plus l'hypothèse de leur intégration à grande échelle dans l'économie traditionnelle. Cependant, la solution technologique permet encore une fois de surmonter ces difficultés notamment par le recours à des crypto-monnaies à stabilité renforcée (B).

A. Le placement à l'aune de l'attractivité des crypto-actifs

167.- Le recours aux NFT. Le blanchiment d'argent par l'art est une réalité[274]. En cause, l'anonymat des acheteurs, l'absence de plus en plus fréquente d'intermédiaire et le caractère hautement spéculatif des œuvres d'art. Or, dans le champ de l'art moderne, les jetons non fongibles

[272] "Qu'est-ce qu'une monnaie fiat ?" Crypto Actu.com, 16 novembre 2022, consulté le 1 janvier 2023.
[273] Toutefois, certains pays comme le Salvador ou la République centrafricaine reconnaissent des crypto-monnaies comme monnaies officielle de substitution, ce qui marque l'hétérogénéité des approches à l'égard de ces technologies comme il le sera précisé au paragraphe XX
[274]M.FERRARI , « Art et blanchiment d'argent », *Sécurité globale*, 2016/3 (N° 7), p. 121-126.

prennent une place grandissante et sont désormais considérés comme des œuvres d'art 3.0[275]. Ainsi, au premier trimestre 2021, les transactions sur NFT auraient représenté près de 1,5 milliards de dollars soit 7,5 % des 20 milliards de dollars rapportés par le marché de l'art en général[276]. Au regard de la place grandissante de ces biens immatériels, des investissements dans des œuvres d'art représentées par des NFT pourraient être mis en place par les organisations criminelles pour dissimuler l'origine de leurs fonds. En effet, par l'acquisition de ces jetons au moyen du produit d'une infraction, il est possible d'effectuer une plus-value importante en le revendant à son tour. En l'absence d'autorité chargée de procéder à ces transactions - qui sont réalisées par la blockchain - celles-ci sont occultes. Par conséquent, des schémas d'auto-blanchiment de capitaux apparaissent avec une décomposition entre l'achat des NFT ou leur génération ex nihilo, leur revente contre des crypto-monnaies et l'intégration finale de ces crypto-monnaies dans l'économie réelle.

168.- La plasticité du Métavers au service du blanchiment. L'univers augmenté soulève également des problématiques en matière de criminalité de conséquence en raison de son tropisme libertarien. L'avantage et l'inconvénient du Métavers est en effet d'être dépourvu de tout encadrement légal ou réglementaire. Il correspond à une réalité parallèle au monde réel et dotée de ses propres modes de fonctionnement, y compris économiques. Or, comme "l*a criminalité ne connaît aucune frontière, que l'espace soit réel ou virtuel, ce qui prime est l'intérêt du gain*[277]*",* il semble naturel qu'elle se soit également appropriée ce nouveau support.

169.- L'économie dans le Métavers repose principalement sur les crypto-monnaies. Les biens s'y acquièrent et s'échangent sans intervention extérieure dans le cadre d'un microcosme dématérialisé. Or, le marché de l'immobilier virtuel à atteint des sommets spéculatifs suscitant l'engouement d'investisseurs de tous horizons[278]. Dès lors, à l'instar du placement d'argent illicite dans le secteur immobilier classique - qui reste l'une des méthodes les plus usitées - il serait possible de voir se reproduire ces opérations dans le monde virtuel en y ajoutant les caractéristiques qui en assurent le fonctionnement. La faiblesse précédemment évoquée du caractère a-territorial de la blockchain sera ici exacerbée en ce que le Métavers est, par définition, au-delà du monde. Aussi, l'origine des fonds investis disparaîtra au profit de l'anonymat.

---

[275] "L'Art NFT : des tableaux 3.0 cryptés et immatériels", Crypto-métaverse.info, 9 août 2022, consulté le 1er janvier 2023.
[276] "Study of the Facilitation of Money Laundering and Terror Finance Through the Trade in Works of Art", *Department of the Treasury,* février 2022.
[277] P. PERROT, "Le métavers : un nouvel univers, une nouvelle criminalité !", *Institut Europia*, novembre 2021.
[278] Certains terrains dans le Métavers ont par exemple pu atteindre 450 000 dollars

B. L'intégration au prisme de la volatilité des crypto-actifs

170.- L'une des limites au développement des crypto-monnaies est leur volatilité. En raison de l'absence de marché réglementé, ces actifs connaissent des évolutions parfois substantielles - tant à la hausse qu'à la baisse. Or, de ce contexte d'incertitude résulte un frein à l'intégration des crypto-monnaies dans le secteur financier traditionnel par les blanchisseurs. Ne parvenant pas à récupérer la valeur investie initialement, ils préféreront conserver ces actifs dans l'espoir de les voir de nouveau atteindre des sommets. Se retrouve la motivation première de ces organisations qui est la recherche de profits.

171.- Le risque induit par les stable coins. Il existe cependant des crypto-monnaies ayant une volatilité moindre, voire nulle, en raison de leur assise sur un valeur sous-jacente solide. Généralement, ces sous-jacents sont des devises légales telles que l'euro, le dollar, le yuan ou le yen. Mais il peut également s'agir de matières premières et notamment l'or[279]. "*Au fondement de la notion de stablecoin (SC) se trouve ainsi la volonté de concilier deux mondes : celui de la monnaie légale, dont les attributs essentiels sont l'ordre hiérarchique, la vocation à l'unicité et la stabilité du pouvoir d'achat, et celui des crypto-actifs (CA), caractérisés par la décentralisation, le foisonnement donc la possibilité de choix, et l'instabilité de leur valeur*[280]*"*. Forts de cette stabilité garantie, les acteurs du blanchiment de capitaux trouveraient dans ces actifs des moyens perfectionnés pour réinvestir les crypto-monnaies dans les monnaies fiat : il leur suffirait de convertir des actifs instables en stable coins avant de vendre ces derniers à un prix conforme à leurs attentes. Par ailleurs, en procédant à cet échange préalable, ils créeraient une couche supplémentaire d'occultation de la nature des fonds blanchis.

[279] "Stablecoin, tout savoir sur ce type de cryptomonnaie", Cryptoast.fr, 9 décembre 2022, consulté le 22 décembre 2022.
[280] A. MELACHRINOS, C. PFISTER, "Stablecoins : le meilleur des mondes ?", *Revue française d'économie*, 2020/4 (Vol. XXXV), p. 23-57.

Paragraphe 2. Le blanchiment « crypto to crypto »

172.- La fongibilité des crypto-monnaies leur confère une capacité de mutabilité particulièrement élevée. Les actifs numériques peuvent être indifféremment échangés contre d'autres actifs de même nature ou d'une autre variété et ainsi alimenter les transactions entre portefeuilles de compositions variables. C'est d'ailleurs ce qui les rapproche de l'argent liquide et donc d'une véritable monnaie. Cette efficacité transactionnelle est cependant favorable au blanchiment d'argent et plus précisément à l'étape de l'empilage - ou de conversion. Une crypto-monnaie, acquise avec de l'argent sale, pourra ainsi avoir connu plusieurs échanges au sein de la blockchain, rendant sa provenance plus opaque.

173.- Pour accroître cette insaisissabilité, il existe des techniques propres à la blockchain permettant de mélanger les crypto-actifs entre eux au sein d'un même portefeuille. Elles reposent sur une mise en commun des actifs d'origines diverses et aboutissent à un obscurcissement de leur provenance (A). En parallèle, il est aussi possible de faire transiter des crypto-monnaies différentes sans avoir à recourir à des portefeuilles distincts. Il s'agit alors de relier deux blockchains dans le cadre d'une même opération (B).

A. Le "mixage" des crypto-monnaies, nouvelle forme d'empilage

174.- Le principe des "mixeurs" de crypto-monnaies consiste à mélanger au sein d'un portefeuille dédié de crypto-monnaies - comme le bitcoin - plusieurs autres crypto-monnaies provenant d'autres portefeuilles. Une fois cette étape réalisée, les crypto-monnaies sont de nouveau réparties entre les différents propriétaires, au prorata de leur dépôt initial. La technique est donc a priori simple, voire simpliste, et repose uniquement sur la fongibilité. Toutefois, elle permet de pallier l'absence d'anonymat de la plupart des actifs numériques, ce qui intéresse nécessairement les acteurs du blanchiment. Ces derniers pourront ainsi blanchir leur crypto-monnaies directement en mélangeant les fonds illicites à des fonds licites.

175.- La faille de ce système est qu'il repose le plus souvent sur des plateformes spécialisées[281]. Celles-ci offrent alors un service de mixage en ligne moyennant une faible commission. Leur intermédiation se justifie par la complexité de recourir à cette technique qui mobilise plusieurs portefeuilles de crypto-monnaies. Or, l'existence de ces plateformes identifiées constitue le point d'entrée des autorités de contrôle et de poursuites dans la lutte contre le blanchiment d'argent. En ce sens, plusieurs intermédiaires ont pu être mis en cause et condamnés pour leur contribution à des actions de blanchiment de capitaux par mixage[282]. Au surplus, ces plateformes peuvent être assujetties aux normes dites LCB-FT et par conséquent astreintes à un devoir de vigilance et de déclaration de soupçons en ce qu'elles peuvent être qualifiées de prestataires sur actifs numériques[283]. Néanmoins, le risque n'est pas nul avec cette technique lorsque le mixage est décentralisé et ne repose donc pas sur l'existence d'une plateforme soumise à un contrôle.

B. L'interopérabilité des blockchains comme catalyseur du blanchiment

176.- Par principe, chaque blockchain est indépendante et incompatible avec tout autre. Cela implique qu'il n'est pas possible d'échanger des bitcoins avec des éthers[284] et inversement au sein d'une seule blockchain. S'il est possible de posséder plusieurs actifs de nature différente, c'est par la création de plusieurs portefeuilles uniques rattachés à une blockchain dédiée. Ainsi, si un individu veut acheter des éthers avec des bitcoins, il devra d'abord vendre ses derniers afin d'acheter les éthers[285]. C'est la raison pour laquelle des "passerelles" ont été conçues entre les différentes chaînes de bloc afin de les rendre interopérables et permettre l'échange de crypto-monnaies différentes. Ce faisant, elles constituent une forme possible de conversion des actifs numériques rapide et simplifiée. Un bitcoin acquis avec des fonds provenant d'un trafic de stupéfiants pourra par exemple être échangé contre un éther. Ce transfert d'une blockchain à l'autre empêchera de retracer la trajectoire de cet actif car celui-ci sera détaché de son support originel. Même si le recours à des plateformes est, à l'instar des mixeurs, fréquemment observé, rien n'exclut

[281] Selon l'article de C. CHENAIS, "Qu'est-ce qu'un mixer de Bitcoin et comment est-ce que ça fonctionne ?", France Crypto.fr, du 12 mai 2021 : *" les plus connues sont Wasabi Wallet, BitcoinMixer, Smartmixer, Blender, BitMix, ChipMixer, CryptoMixer ou encore FoxMixer"*.

[282] Ainsi en 2020, les autorités belges et néerlandaises ont coopéré sous la supervision d'Europol afin de faire fermer l'une des plateformes de mixage les plus importantes - Bitmixer.io - accusée d'avoir permis le blanchiment de 200 millions de dollars sur l'année in "Europol ferme un des plus grands mixeurs de cryptos mondiaux pour blanchiment de fonds", Cryptoast.fr, 19 avril 2020, consulté le 22 décembre 2022.

[283] Ces PSAN sont en effet visées par l'article L.561-2 du Code des marchés financiers au titre des entités soumises aux obligations du présent chapitre.

[284] Crypto-monnaies de la blockchain Ethereum.

[285] "Qu'est-ce qu'une passerelle blockchain ?", Binance Academy.com, 11 novembre 2022, consulté le 12 décembre 2022.

que les organisations criminelles choisissent de s'en passer et d'utiliser des passerelles "non custodial[286]".

177.- Le poids de la blockchain dans le blanchiment de capitaux est significatif. Selon le dernier rapport de l'entreprise Chainalysis, il représenterait entre 2017 et 2021 près de 33 milliards de dollars[287]. Cette technologie est par essence profilée pour faciliter la dissimulation des activités économiques criminelles et assurer l'impunité de ses auteurs[288]. Cependant, par comparaison avec la valeur totale du blanchiment d'argent - estimée par ce même rapport entre 800 milliards et 2000 milliards de dollars par an - la part représentée par la blockchain semble marginale. Le risque est pourtant de ne pas y attacher suffisamment d'importance et de ne pas mobiliser tous les moyens nécessaires pour l'endiguer. Or, saisir le mal à la racine avant qu'il ne s'installe trop profondément est une exigence que les États doivent assumer. Il en va de la confiance dans la blockchain et de sa crédibilité dans le cadre d'un usage bénéfique.

Conclusion de la première partie

178.- Vers une conceptualisation de la criminalité liée à la blockchain. L'approche de la blockchain par le prisme de son caractère potentiellement criminogène aboutit à une mise en avant des infractions dont elle peut être à la fois le vecteur et la cible. Malgré un effort d'exhaustivité, cette présentation ne saurait rendre compte de tous les phénomènes criminels - présents et à venir - sous-tendus par cette technologie. C'est donc plus une tentative de conceptualisation des particularismes de cette criminalité 3.0 qui a été esquissée qu'une définition approfondie - laquelle apparaît en l'état des connaissances sur le sujet impossible.

179.- Une criminalité anonyme et internationale. Ces deux aspects ont servi de fil rouge pour les développements précédents. Elles constituent les principales difficultés et par conséquent les

[286]Ibid, *" Les passerelles non custodial fonctionnent de manière décentralisée, en s'appuyant sur des smart contracts pour gérer les processus de verrouillage et d'émission crypto, éliminant ainsi le besoin de faire confiance à un opérateur centralisé".*
[287] Rapport Chainalysis : « Crypto-crime 2022 », p. 11.

[288]A.ALBERTINI , "Cryptomonnaies : les cyber gendarmes démantèlent une plate-forme de blanchiment", Le Monde, 19 janvier 2022, consulté le jour même : *"Bitzlato, dont au moins un hébergeur se situait en France, d'après le parquet de Paris, se targuait de ne réclamer à ses clients « ni selfie ni passeport », selon la justice américaine, et fonctionnait comme un véritable service en ligne de blanchiment de crypto actifs : les criminels y injectaient le produit de leurs activités illicites, la plate-forme se chargeait d'opacifier leur provenance, moyennant une commission de l'ordre de 5 %, avant de les réintroduire dans le circuit des crypto monnaies pour un nouveau cycle de blanchiment, ou n'importe quel usage ultérieur. Elle proposait aussi de les convertir en roubles".*

principaux défis que soulèvent la blockchain. Saisies par les organisations ou des acteurs isolés, elles offrent une potentialité de nuisance substantielle et obligent à reformuler les règles traditionnelles qui irriguent le droit pénal de fond et de procédure. L'anonymat dont il a été pourtant précisé le caractère relatif suscite des enjeux d'identification des infractions mais également d'attribution de la responsabilité. En ce que pour lutter contre une forme de criminalité il faut pouvoir la comprendre, un effort - voir un saut - technologique devra être entrepris par les autorités de poursuites. L'internationalisation de la blockchain représente quant à elle une problématique d'ordre procédural liée à l'absence d'uniformisation des instruments internationaux de prévention et de répression ainsi qu'à la nécessaire collaboration opérationnelle qu'elle implique. Dans cette situation, c'est sur la base d'une décentralisation de la lutte que la réponse pourra être apportée.

180.- Une approche nécessairement prospective. En effet, eu égard à la faible épaisseur temporelle de la blockchain et de ses applications, la présentation proposée est placée sous le sceau de l'incertitude ou plus précisément de l'absence de certitude. Bien que des études scientifiques aient été produites sur le sujet[289], elles concernent surtout les usages de la blockchain dans des domaines scientifiques ou commerciaux. Dans le champ de droit, ses particularismes sont généralement présentés sous l'angle du droit civil ou financier. Le droit pénal semble dans ce cadre moins sensible à cette technologie en raison de ses fondements que sont les principes de légalité et de territorialité, lesquels apparaissent peu miscibles dans la blockchain. Cependant, les infractions détaillées permettent de réfuter cette première analyse et ce par le truchement de leur appréhension et de leur qualification constructive par le juge. Ce pouvoir prétorien est - comme souvent en matière répressive - indispensable à l'adaptation de la réponse pénale à des nouvelles formes de criminalités pour lesquelles le législateur est tout d'abord dépassé. Mais parce qu'un État de droit ne saurait reposer exclusivement sur la jurisprudence, ces enjeux doivent être définis avec le plus haut niveau de précision que permettent la législation et la réglementation. Dès lors, c'est vers une évolution du droit répressif pour lutter contre l'émergence de la blockchain qu'il faudra aller.

[289] Ainsi, 528 000 résultats apparaissent pour l'occurrence "blockchain" sur le moteur de recherche Google Scholar, ce qui ne correspond qu'à une partie de l'ensemble de la recherche.

Seconde partie. La nécessaire évolution du droit répressif face à la technologie blockchain

181.- La blockchain est une forme perfectionnée de décentralisation de la technologie. Elle se veut la plus accessible et la moins contraignante possible dans son utilisation. À ce titre, elle est susceptible d'être utilisée par une partie croissante de la population, répondant en cela à l'attrait plus général de l'humanité vers les nouvelles technologies[290]. Or, à tout phénomène mondial correspond une réponse mondiale. L'appréhension de cette technologie impose donc aux États d'agir de concert et non pas de s'ériger en défenseur d'un souverainisme de mauvais aloi. Le droit pénal international et le droit international pénal sont des exemples de concessions faites dans un domaine pourtant inhérent à la souveraineté nationale. Il doit en être de même pour la criminalité liée à la blockchain.

182.- Unis dans la diversité[291], les États n'en sont pas moins des concurrents sur le plan économique, voire politique. Dès lors, promouvoir une réponse internationale face à un dispositif aussi prometteur que la blockchain risque de se heurter à la realpolitik. De plus, en ce qu'elle repose sur le concept de cyberespace[292], elle ne peut être cantonnée aux seules frontières territoriales. Son champ de rayonnement est au contraire universel si bien qu'aucun État, même le plus puissant, ne saurait seul l'appréhender. C'est donc la raison de l'exigence aiguë d'une coopération interétatique comme fondement de la réponse internationale apportée à la criminalité liée à la blockchain (**Titre I**).

183.- Le choc technologique résultant de l'extension de l'usage criminel de la chaîne de blocs aboutit à une remise en question des processus traditionnels de prévention et de répression. La dynamique de cette nouvelle criminalité est avérée et les limites capacitaires des États éprouvées. Partant, pour qu'une réaction efficace ait lieu, la réponse à la modernisation des infractions doit être la modernisation correspondante des concepts centraux du droit répressif. Au-delà de l'amélioration

[290] Dans son rapport *"L'ère de l'interdépendance numérique"* de juin 2019, le Groupe de haut niveau sur la coopération numérique de l'ONU précise que "*les technologies numériques ont touché près de la moitié de la population mondiale"*. Bien qu'il soit nécessaire de tempérer cette proportion qui ne prend pas en compte le niveau de développement de ces technologies, elle révèle toutefois l'omniprésence de ces outils numériques dans le quotidien de nombreux individus.
[291] Devise de l'Union européenne.
[292] Voir à ce sujet le premier paragraphe de la première partie.

de la répression, c'est également sur le sentiment d'insécurité - lié à la méconnaissance de ces nouveaux comportements - que les États peuvent travailler et ainsi diminuer les risques de remise en cause illégitimes d'une technologie a priori vertueuse.

184.- La faculté d'adaptation des espèces a été au cœur de l'histoire naturelle. La théorie de l'évolution de Charles DARWIN explique bien que "*toutes les espèces vivantes sont en perpétuelle transformation et subissent au fil du temps et des générations des modifications morphologiques comme génétiques*[293]*"*. Plus précisément, "*les espèces qui survivent ne sont pas les espèces les plus fortes, ni les plus intelligentes, mais celles qui s'adaptent le mieux aux changements"*[294]. Appliquée aux États, cette assertion signifie que leur survie dépend moins de leur puissance intrinsèque que de leur aptitude à remettre en question leur ethos et en s'adaptant à leur environnement. Aussi, pour pouvoir lutter efficacement au niveau national contre la criminalité commise par ou contre la blockchain, la réponse pénale - monopole étatique ? - devra reposer sur l'adaptation (**Titre II)**.

Titre I. Une réponse internationale fondée sur la coopération

185.- Une réflexion globale pour une action globale ? La question du niveau de conceptualisation de l'approche pénale suscite les sempiternelles questions du niveau territorial le plus adéquat pour agir. Lorsque le phénomène est susceptible de recevoir une acception nationale, c'est cette strate qui doit être privilégiée selon un principe de subsidiarité[295]. Mais lorsque la seule réponse interne n'est pas suffisante pour apporter une solution à des problématiques qui la dépassent, la coopération se fait nécessaire.

186. - Deux cadres de coopération interétatique peuvent être distingués. Selon l'approche la plus large et la moins intégrée, la coopération peut se faire au niveau international. Dans ce contexte, elle sera d'autant plus complexe que la multiplication des régimes juridiques et politiques aboutira à une hétérogénéité dans l'approche initiale du la blockchain. Celle-ci variera en effet d'un pays à l'autre au gré des conditions sociales, économiques et politiques. Mais, une fois surmonté cet

[293] E. FERARD, "Charles Darwin : qu'est-ce que la théorie de l'évolution ?", Geo.fr, 11 février 2022, consulté le 22 décembre 2022.
[294] C. DARWIN, *L'Origine des espèces,* 1859.
[295] Selon le Glossaire du droit international, *"le principe de subsidiarité est une règle de répartition des compétences entre l'Union européenne et ses Etats membres. En dehors des domaines de compétences qui lui sont propres, l'Union Européenne n'agit que si son action est plus efficace que celle conduite au niveau des Etats ou des régions".* Bien que pensé à l'échelle de l'Union européenne, ce principe peut néanmoins s'appliquer à l'échelle internationale.

obstacle conceptuel, une approche, sinon commune à tout le moins harmonisée, serait possible. Cette coopération internationale sera la forme minimale pouvant renforcer l'efficacité de la lutte (**Chapitre 1**).

Dans une dimension plus réduite mais également plus intégrée, la coopération européenne constitue l'autre forme de coopération entre États permettant une réponse répressive non plus seulement harmonisée mais commune. Elle s'inscrit dans l'ADN de l'Union européenne, lequel lui donne une physionomie quasi-fédérale. Les dernières limites à l'intégration européenne empêchant pour l'heure de pouvoir concevoir une action unique de l'entité européenne, la coopération renforcée qu'elle met en place apparaît cardinale dans la lutte contre cette forme de criminalité 3.0 (**Chapitre 2**).

Chapitre I. La coopération internationale, socle minimal d'une action collaborative de lutte contre la criminalité blockchain

187.- Pour traiter d'une problématique encore faut-il que celle-ci soit définie dans des termes analogues par chaque acteur. Sans ce travail initial, l'adoption d'une solution commune est rendue infiniment complexe. De même et au-delà de la seule définition des termes du débat, le traitement politique et juridique de la situation par les différents protagonistes ne doit pas être contradictoire, aux risques d'obérer toute possibilité d'y apporter une solution en collaborant. La blockchain est à cet égard source de difficultés dès lors qu'il s'agit par nature d'un dispositif clivant. Elle n'est pas assez ancienne à l'échelle de l'histoire des relations internationales pour faire l'objet d'un consensus[296]. Il est pourtant requis de la part des États qu'ils se mettent d'accord pour lutter efficacement ensemble contre les infractions permises par cette technique. Aussi, la recherche d'une vision convergente dans la lutte contre la criminalité blockchain sera un préalable obligatoire (**Section 1**).

188.- Une fois ce consensus obtenu, la mise en œuvre effective de la politique internationale de lutte devra être mise en œuvre par des actes concrets. À ce niveau territorial, il semble permis

[296] Le consensus désigne à la fois une procédure d'adoption d'un accord et le résultat de cette procédure. Il fut d'abord utilisé dans le cadre de l'Onu avant d'être progressivement étendu à d'autres organismes internationaux ou régionaux tels que l'Union européenne selon H. CASSAN. *Le consensus dans la pratique des Nations Unies.* In: *Annuaire français de droit international*, volume 20, 1974. pp. 456-485.

d'exiger de la part des États qu'ils se coordonnent afin d'orienter leur action répressive dans une même direction. Cette convergence dans la lutte contribuera à l'aspect opérationnel de la coopération internationale (**Section 2**).

Section 1. La recherche d'une vision convergente dans la lutte contre la criminalité blockchain

189.- Mettre en avant la nécessaire convergence des acceptions de la blockchain et de ses éléments suppose que soit constatée au préalable une certaine divergence. Or, ces divergences peuvent prendre de multiples formes et reposer sur des justifications distinctes. Cependant, parmi toutes ces approches, deux grandes catégories peuvent être mises en lumière tant leurs antagonismes semblent profonds. Aussi, la première étape de l'harmonisation conceptuelle sera de cerner ces différences (**Paragraphe 1**). Une fois que les différentes conceptions de la blockchain seront connues - du moins dans leurs idées les plus fortes - il faudra tenter de réduire au maximum ces dissensus. Pour ce faire, l'adhésion volontaire du plus grand nombre sera la clef de voûte du système. Or, pour obtenir l'accord le plus large sur une idée de la blockchain, celle-ci doit être conçue de manière suffisamment compréhensive. Le cadre international sera le niveau de réflexion retenu. Le groupe d'action financière sera l'acteur de rapprochement choisi (**Paragraphe 2**).

Paragraphe 1. Des approches disparates face à la blockchain

190.- L'appréhension de la technologie blockchain varie d'un pays à l'autre. Relevant de choix de souveraineté, les technologies sont rarement saisies de manière uniforme par les législations nationales. Toutefois, cette absence de consensus peut en principe ne poser de problèmes que d'ordre économique et commercial lorsque les instruments en cause ne suscitent pas de débat d'intérêt général. Mais lorsque de ces conceptions dépendent des enjeux de sécurité et d'ordre public, il résulte de ces incompréhensions un risque plus prégnant.

191.- Deux approches radicales peuvent être distinguées à l'égard d'une innovation. Dans une première, qualifiée de libérale, l'État tolère, voire promeut cette nouveauté en pensant pouvoir en exploiter les fruits. Il s'agit généralement de pays à développement élevé dont les ressources sont

plus intellectuelles que matérielles. En ce qui concerne la blockchain et ses dérivés, une telle approche s'entend de son admission totale ainsi que d'une utilisation dans de nombreux champs de la vie économique et sociale. Cependant, il importe de se demander si ce choix de la tolérance n'est pas en fait un vecteur d'impunité pour certains comportements contraires à l'intérêt général (A).

Dans une seconde acception, opposée à la première, le choix est celui d'un encadrement strict des technologies les plus récentes ou les plus influentes. À ce titre, le sort de la blockchain oscille généralement entre régulation étroite et interdiction formelle. Mais, là encore, cette radicalité n'est pas synonyme de sécurité. Bien au contraire, l'excessive restriction peut générer des stratégies de contournement et d'externationalisation (B).

A. Le choix de la tolérance face au risque d'impunité

192.- L'exemple du Salvador ou "l'Eldorado du bitcoin". Le 7 septembre 2021, le Salvador est devenu le premier pays au monde à faire du bitcoin une monnaie légale au même titre que le dollar. Désormais, les Salvadoriens peuvent *"effectuer des paiements en ligne ainsi qu'envoyer ou recevoir de l'argent vers et/ou de l'étranger à des frais pratiquement inexistants[297]"*. Il s'agit donc de l'approche la plus extensive possible du bitcoin consistant à le traiter comme une monnaie légale. Ce choix de société, de nature politique, constitue un exemple quasiment unique au monde[298]. Or, il est intéressant de souligner que le Salvador est également un paradis fiscal reconnu et qu'il attire ainsi les investissements illicites[299]. Dès lors, la question qui se pose est celle de savoir si l'acceptation du bitcoin comme devise aura un effet notable sur les différents procédés d'évasion fiscale, voire de blanchiment de capitaux.

193.- Contourner les sanctions financières internationales par la blockchain. Les sanctions internationales sont *"un ensemble des mesures diplomatiques, économiques ou militaires prises par un Etat ou par une organisation internationale pour faire cesser une violation du droit international qu'une organisation a constatée ou dont un État s'estime victime[300]"*. Elles peuvent être de

[297]A. REUTER, *Rôle du Bitcoin sur les marchés financiers : Analyse de ses propriétés et de son potentiel rôle de valeur refuge,* Mémoire de recherche à l'Université de Namur, 2022.
[298]Depuis le 3 juillet 2022, le République centrafricaine à également adopté le bitcoin comme monnaie légale aux côtés du Franc CFA.
[299] J. FONTANEL. Le crime international organisé et les cryptomonnaies. "Les Géopolitiques" de Brest, Université de Bretagne Occidentale (UBO); IMT Atlantique; ENSTA Bretagne; École navale, Feb 2022, Brest, France.
[300] *ABC du droit international public*, p.34.

différentes natures et notamment financières. Dans ce cadre, elles consistent parfois en des gels d'avoirs de personnalités impliquées dans des violations des droits de l'Homme, des saisies de biens situés à l'étranger ou encore l'exclusion de certains marchés financiers. À la suite de l'invasion de l'Ukraine par la Russie le 24 février 2022, de nombreuses sanctions financières ont été fulminées à son encontre[301]. Or, la cryptomonnaie est susceptible d'affaiblir l'effet escompté. Certains[302] ont tout de suite saisi les risques induits par ces actifs intraçables et échappant à tout contrôle étatique. Le risque majeur en effet est que les interdictions financières auxquelles la Russie est soumise et qui ne concernent que les devises légales ne soient contournées par le recours à des transactions en bitcoin[303]. Si l'Union européenne a explicitement inclus les crypto-monnaies dans le champ des sanctions[304] et a par la même exigé des entités émettrices et réceptrices d'opérer les contrôles ad hoc, il est permis de douter de l'efficacité d'une telle précaution. En effet, le propre de la blockchain étant la décentralisation et l'anonymat, elle peut ainsi aboutir à des échanges imperceptibles au niveau international. Par conséquent, la maille de la surveillance risque d'être trop large pour saisir de tels échanges et il est certain que la Russie continue de se faire financer en partie par des crypto-monnaies[305].

194.- Une utilisation salutaire de la blockchain est également possible. La guerre en Ukraine est un exemple topique des paradoxes qu'offre la technologie de la chaîne de blocs. Employée afin d'alimenter financièrement l'envahisseur, elle peut en parallèle être une source d'aide humanitaire. Les projets de levées de fonds au moyen des NFT se sont multipliés depuis le début du conflit avec par exemple la vente d'un jeton représentant le drapeau ukrainien pour 6,5 millions de dollars en ETH[306]. De même, l'Ukraine ayant adopté une politique de large admission des crypto-monnaies[307], elle reçoit une grande partie de ses soutiens matériels par le biais de cet instrument. Le gouvernement ukrainien a d'ailleurs communiqué sur Twitter l'adresse de ses portefeuilles crypto[308].

---

[301] Selon l'état des lieux dressé par le ministère de l'Europe et des Affaires étrangères d'octobre 2022, la Russie a notamment fait l'objet d'une interdiction de transaction sur les avoirs et réserves de sa Banque centrale, et plusieurs institutions bancaires russes ont été exclues du réseau SWIFT facilitant les transactions internationales.
[302] Lettre des sénateurs démocrates au Trésor public américain, 2 mars 2022 in A. LEJNIECE, « Les crypto-monnaies au cœur de la guerre de la Russie contre l'Ukraine », *RED*, 2022/1 (N° 4), p. 78-83.
[303] *Ibid*, la lettre fait état à titre d'exemple d'une précédente utilisation de bitcoins par la Corée du Nord et l'Iran pour soutenir leur projet militaires respectifs nonobstant les sanctions économiques dont ils faisaient l'objet.
[304] Règlement (UE) 2022/394 du Conseil du 9 mars 2022 modifiant le règlement (UE) n° 833/2014 du Conseil du 31 juillet 2014, article 1, paragraphe 1, point f)
[305] N. AÏT-KACIMI, "La Russie capte 120 milliards de dollars en bitcoin et cryptos", *Les Échos*, 13 octobre 2022, consulté le 12 décembre 2022.
[306] *Op cit,* A. LEJNIECE.
[307] L'Ukraine a d'ailleurs légalisé les crypto-monnaies le 17 février 2022 ce qui renforce sa position d'ouverture en la matière.
[308] *Ibid*.

B. Le choix du tout répressif et le risque d'externationalisation de la criminalité

195.- A contrario, d'autres pays ont décidé d'encadrer la technologie blockchain de manière extensive. L'exemple le plus représentatif est celui de la Chine. En effet, le géant asiatique a fait le choix d'interdire à ses institutions le commerce de crypto-monnaies. Elle justifiait son choix par les risques induits par ces vecteurs de fraude, blanchiment ou autres actions prohibées[309]. Toutefois, cette approche est paradoxale car la Chine dispose de sa propre blockchain et de sa propre crypto-monnaie : le e-yuan. Dès lors, il faut plutôt considérer que ce pays a opté pour une nationalisation de la blockchain et par conséquent une interdiction des autres technologies analogues. Ce quasi-monopole n'en est pas moins source d'interrogations.

196.- L'effet plumeau[310] appliqué à la criminalité 3.0. Il est désormais démontré que lorsqu'un phénomène criminel est appréhendé par des moyens préventifs - vidéosurveillance - ou répressifs - systématisation des poursuites pénales - les auteurs de ces actes cherchent à en pérenniser la commission tout en évitant la sanction. Pour cela, ils recourent à un déplacement de leur activité dans des lieux dépourvus de contrôle. Ce fait criminologique a été observé notamment pour le trafic de stupéfiant ou les atteintes aux biens. Il pourrait l'être également pour la criminalité blockchain. En raison des divergences nationales s'agissant de son contrôle, la tentation sera grande d'externaliser la criminalité dans des pays plus ouverts.

197.- L'utilisation de blockchain étatique, un risque pour les droits fondamentaux ? En excluant la blockchain en général tout en créant sa blockchain particulière, la Chine s'est lancée dans un projet d'extension du contrôle social de sa population. En exploitant son caractère de registre immuable et extensif, Pékin a initié une centralisation des informations individuelles de ses citoyens[311]. Couplée à des smarts contracts pour automatiser le traitement des données, ainsi qu'à l'emploi du "crypto-yuan" pour suivre les transactions effectuées, le pays est en passe de devenir

[309] S. MAMMAR, *Le Bitcoin peut-il être considéré comme une valeur refuge au vu de sa volatilité,* Mémoire de recherche à l'Université de Namur, 2022.
[310] K. J. BOWERS , S. D JOHNSON, "Measuring the geographical displacement and diffusion of benefit effects of crime prevention activity", *J. Quant. Criminol.*, 19, 275–301, 2003.
[311] F.BAYARD, "La blockchain, un danger pour la liberté et la vie privée ?", in cryptocat.fr, 20 octobre 2020, consulté le 12 novembre 2022.

une véritable “techno-dictature”[312]. La technologie blockchain semble être l’outil parfait pour atteindre les finalités coercitives de la Chine et notamment l’amélioration de son système de crédit social[313], par recoupement de toutes les informations et leur suivi en temps réel. Elle ouvre ainsi la voie à des usages attentatoires aux droits fondamentaux tels que le respect de la vie privée ou les libertés individuelles. L’évaluation de ses effets concrets est encore prématurée mais doit être évoquée afin de s’y préparer. Des pays autoritaires sont à ce titre de bons exemples de ce qu’il faut craindre dans l'utilisation dévoyée de la blockchain.

C. Le positionnement de la France, entre encouragement de l’innovation et encadrement des activités

198.- En France, la prise en compte de la blockchain par les pouvoirs exécutif et législatif fut précoce par rapport aux autres pays de l’Union européenne. Dès 2016[314] en effet, un premier encadrement de la blockchain a été établi lui donnant une première définition dans le Code des marchés financiers[315]. Mais c’est par la loi pour la croissance et la transformation économique des entreprise dite loi PACTE du 22 mai 2019 que le législateur a pris pleinement en compte cette nouvelle technologie en encadrant plus particulièrement les *Initial coin offering*[316] (ICOs) - sur le marché primaire - et en supervisant plus étroitement les prestataires de service sur actifs numériques - sur le marché secondaire[317]. Ces deux étapes de la circulation des actifs que sont leur création - par les ICOs - et leur échange - par les PSAN - ont par ailleurs été encadrées de manière différenciée.

199. S’agissant des ICOs, la loi PACTE précitée prévoit d’assujettir les émetteurs à un visa optionnel de l’AMF “*permettant de prouver leur sérieux et la qualité de leur offre*[318]*”*. Il ne s’agit donc pas d’une obligation mais d’un simple label de conformité. Or, ce caractère simplement

---

[312] “De l’usage de la blockchain en Chine comme outil de surveillance. Un modèle exportable ?” Cryptoactu.fr, 20 janvier 2020, consulté le 12 novembre 2022.

[313] *Ce projet du gouvernement chinois vise à mettre en place un système national de réputation des citoyens et des entreprises en y ajoutant un système de récompenses et de pénalités pour ceux respectant ou ne respectant pas les règles édictées Chacun d'entre eux se voit attribuer une note, échelonnée entre 350 et 950 points dite « crédit social », fondée sur les données dont dispose le gouvernement à propos de leur statut économique et social”,* R. RAPHAËLLE et L.XI, « Bons et mauvais Chinois : Quand l’État organise la notation de ses citoyens »*, Le Monde diplomatique, janvier 2019.*

[314] Ordonnance n° 2016-520 du 28 avril 2016 relative aux bons de caisse.

[315] C. mon.fin., art. L.223-12 : *“sans préjudice des dispositions de l'article L. 223-4, l'émission et la cession de minibons peuvent également être inscrites dans un dispositif d'enregistrement électronique partagé permettant l'authentification de ces opérations, dans des conditions, notamment de sécurité, définies par décret en Conseil d'Etat”*

[316] Voir la définition donnée au n° 22-1 sur l’escroquerie.

[317] *Rapport d’information sur la mise en œuvre des conclusions de la mission d’information relative aux crypto-actifs,* présenté par Eric WOERTH et enregistré à l'Assemblée nationale le 1er décembre 2021.

[318] Ibid.

facultatif semble dommageable en ce que la délivrance du visa est subordonnée au respect de la règlementation LCB-FT, là où le secteur des émissions de jeton est particulièrement sensible au blanchiment de capitaux et financement du terrorisme[319].

190.- Les PSAN font l'objet d'un encadrement plus contraignant. Outre leur assujettissement aux normes LCB-FT[320] à l'instar des autres intermédiaires de services financiers, les prestataires sur actifs numériques doivent en outre être identifiés par les autorités de régulation des marchés financiers et de la concurrence. Plus précisément, le Code des marchés financiers opère une distinction entre les PSAN agissant dans le cadre d'échanges crypto-to-fiat" ainsi que la conservation d'actifs numériques et les autres prestataires. Les premiers doivent en effet obligatoirement s'enregistrer auprès de l'Autorité des marchés financiers - après avis de l'ACPR - laquelle vérifie si plusieurs conditions sont réunies[321], notamment la conformation aux obligations en matière de lutte contre le blanchiment et le financement du terrorisme. Quant aux autres prestataires, opérant sur les autres transactions, ils sont soumis à titre facultatif à un agrément délivré par l'AMF[322]. Or, comme le souligne le rapport parlementaire précité, cette différence de régime fondée sur une distinction opérée initialement par la 5ème directive anti blanchiment de l'Union européenne n'est plus conforme aux nouvelles recommandations du GAFI[323] qui englobent dans le champ d'assujettissement obligatoire aux normes LCB-FT aussi bien les PSAN opérant sur les transactions "crypto-to-fiat" que ceux opérant sur les transactions "crypto-to-crypto". Partant, une harmonisation est préconisée.

191.- Au constat des dispositions par lesquelles la France encadre les activités reposant sur la blockchain doit répondre la conclusion selon laquelle le cadre juridique est développé. Toutefois, afin de renforcer la prévention des activités illicites permises par cette technologie, il paraît nécessaire de le compléter afin de le mettre en cohérence avec celui prévu au niveau international par le GAFI.

[319] Voir les développements relatifs aux techniques de blanchiment au n°137.
[320] C. mon.fin., art. L. 561-2, 7° bis et 7 °quater préc.
[321] C. mon.fin., art. L. 54-10-3, 4°.
[322] C. mon.fin., art. L. 54-3-5.
[323] Voir à cet égard n° 171 et suivants.

Paragraphe 2. Une approche unitaire en construction sous l'égide du GAFI

192.- Le groupe d'action financière ou GAFI est une organisation internationale créée en 1989 à l'initiative du G7 dans le but de prendre des mesures pour améliorer la lutte contre le blanchiment de capitaux au niveau international, avant de voir son action étendue au financement du terrorisme en 2001[324] - après les attentats du World Trade Center. Comptant désormais 39 membres dont la Commission européenne, il agit principalement par voie de recommandations portant sur l'évaluation des enjeux liés à la criminalité économique, son blanchiment et et le financement du terrorisme. Il est donc une source importante de l'action internationale de lutte contre la criminalité et se veut un acteur clef dans l'adaptation des États aux nouvelles formes qu'elle adopte.

193. - Un facteur direct d'harmonisation des réponses nationales. Au regard de son expertise et de l'autorité qui s'attache à ses prises de position, le GAFI est un organe majeur dans l'harmonisation des législations nationales dans le cadre de la lutte contre la criminalité. Il s'intéresse en effet aux phénomènes avérés et émergents afin d'en estimer les risques et de préconiser des solutions pour s'y adapter. Le rôle joué par ses lignes directrices et recommandations est donc fondamental, notamment s'agissant de la définition d'un concept ne faisant pas consensus. Or, comme l'ont montré les développements précédents, la blockchain constitue une technologie clivante souffrant d'un déficit de convergence. En donnant de cette technologie et ses satellites une acception potentiellement commune, le GAFI apparaît ainsi comme l'initiateur d'une réponse pénale internationale homogène (A).

194.- Un catalyseur indirect de la lutte internationale. Mais une fois que les termes en tension ont été précisés, il incombe aux États de faire en sorte que leur arsenal préventif et répressif soit suffisamment étoffé. A cet égard, la fonction du GAFI sera également essentielle. En tant que source de propositions en matière de lutte contre le blanchiment et le financement du terrorisme, il pourra bien évidemment permettre aux États d'améliorer leurs systèmes de lutte en la matière. Mais plus généralement, en ce qu'il dispose d'une vision globale des nouveaux modus operandi criminels, il pourra mettre en lumière les dispositifs innovants capables d'en conjurer l'expansion (B).

[324] GAFI, "Historique du GAFI", disponible en ligne à l'adresse suivante : https://www.fatf-gafi.org/fr/the-fatf/historique-du-GAFI.html

A. Le travail définitoire préalable du GAFI aux fins d'harmonisation de la réponse pénale internationale

195.- Le Groupe d'action financière s'intéresse à la blockchain et plus précisément aux actifs numériques depuis plusieurs années. Dès 2014 en effet, il publiait un guide sur les monnaies virtuelles et les risques associés[325]. Il y décelait déjà les potentiels détournements aux fins de blanchiment d'argent et de financement du terrorisme (2). Mais il commençait aussi par définir les termes du sujet, préalable indispensable pour une compréhension commune à tous les États membres (1).

1. La définition des dispositifs fondés sur la blockchain

196.- La blockchain est moins une technologie isolée que le soubassement fonctionnel de plusieurs dispositifs. Elle connaît de multiples manifestations dont il est nécessaire de connaître les caractéristiques principales. Les plus importantes s'agissant de la criminalité sont les crypto-monnaies, les jetons non fongibles et les prestataires de services sur actifs numériques. Pour ces différents éléments, le GAFI offre une définition censée susciter l'adhésion la plus grande.

197.- S'agissant des crypto-monnaies, le groupe d'action financière parle plus volontiers d'actifs virtuels ou numériques. Il les présente comme *"une représentation numérique d'une valeur qui peut être échangée ou transférée par un moyen numérique et qui peut être employée à des fins de paiement ou d'investissement[326]"*. Cette approche compréhensive se veut par la même évolutive. Face au développement rapide de ces actifs, il est pertinent de ne pas les enfermer dans une acception trop rigide. Cela incitera également les États à adhérer à cette définition peu exigeante.

198. - Les jetons non fongibles sont quant à eux envisagés comme *"des actifs à collectionner qui ne sont pas en eux-mêmes des actifs virtuels[327]"*. Il s'agit là d'établir une distinction entre ces jetons et les autres actifs numériques que sont les crypto-monnaies. Par celle-ci, le GAFI marque bien la différence existante entre d'une part des représentations d'un actif ou d'un objet que sont les NFT et d'autre part, les actifs fongibles et autonomes que sont les crypto-monnaies.

---

[325] "Virtual Currencies: Key Definitions and Potential AML/CFT Risks", FAFT, juin 2014.

[326] "Lignes directrices de l'approche fondée sur les risques appliquée aux actifs virtuels et aux prestataires de services liés aux actifs virtuels", GAFI, 21 juin 2019.

[327] FATF (2021), Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers.

199. - Enfin, les prestataires de service sur actifs numériques sont désormais définis comme étant *"toute personne physique ou morale qui n'est pas visée autre part dans les Recommandations et qui exerce à titre commercial une ou plusieurs des activités ou opérations suivantes pour le compte ou au nom d'une autre personne physique ou morale*[328]", avant de lister les activités exercées que sont les "*échanges entre des actifs virtuels et des monnaies fiduciaires ; échanges entre une ou plusieurs formes d'actifs virtuels ; transfert d'actifs virtuels ; et conservation et/ou administration des actifs virtuels ou des instruments permettant de contrôler les actifs virtuels ; participation à et fourniture de services financiers liés à une offre d'un émetteur et/ou la vente d'un actif virtuel".* Cette dernière définition est salutaire au regard de l'ampleur prise par les plateformes de transaction de crypto-monnaies qui, jusqu'alors, n'étaient pas ou peu encadrées. Elle est, dans le prolongement des autres notions présentées, particulièrement large et englobe toutes les opérations portant sur des actifs numériques. Ce faisant, elle permet d'attirer sous ses latitudes l'ensemble des professionnels du domaine.

2. L'analyse des risques consubstantiels à la blockchain

200.- Dans son office de vigie, le GAFI a une mission d'abord prophylactique. Il établit une catégorisation des risques selon la nature des techniques criminelles potentielles qui résultent du développement de tel ou tel outil. Une fois présenté in abstracto, il évalue le degré de risque pesant sur les États en comparant les dangers existant aux moyens dont ils disposent. Cette évaluation permettant de définir les mesures à adopter pour y répondre[329]. En raison de son coeur de compétence de nature économique et financière, c'est plus précisément dans le domaine du blanchiment de capitaux et de financement du terrorisme que se déploient ses analyses.

201.- S'agissant en particulier de la France, le GAFI se fonde sur l'ANR - Analyse nationale des risques - établie régulièrement par la COLB[330]. Il en déduit s'agissant des risques LCB-FT liés aux crypto-monnaies que le risque est modéré. En effet, malgré des particularités rendant la blockchain potentiellement source de criminalité - anonymat, caractère transfrontalier, régulation et rapidité - il

[328] "Lignes directrices de l'approche fondée sur les risques appliquée aux actifs virtuels et aux prestataires de services liés aux actifs virtuels", préc.
[329] Cette approche par les risques se rapproche de la cartographie des risques que doivent mettre en place certaines entreprises afin de prévenir les faits d'atteinte à la probité. Elle résulte d'une comparaison entre les risques dits bruts - ceux pesant sur l'entreprise - avec les moyens d'y faire face pour in fine aboutir aux risques dits nets restant à traiter.
[330] GAFI (2022), Mesures de lutte contre le blanchiment de capitaux et le financement du terrorism - France, Rapport du quatrième cycle d'évaluations mutuelles

tempère la menace en évoquant le nombre relativement faible de prestataires de service sur actifs virtuels ainsi que leur soumission à un enregistrement auprès de l'AMF[331]. Il souligne aussi le pouvoir de sanction de l'autorité prudentielle et de résolution à l'encontre des PSAV qui ne se soumettraient pas à leurs obligations LCB-FT. Ces dernières sont néanmoins considérées comme des entités à risque. Toutefois, il relève des lacunes s'agissant du respect des normes de vigilance notamment en ce qui concerne l'identité réelle des donneurs d'ordre et des bénéficiaires effectifs de ces PSAV[332] pour lesquels il n'est parfois pas possible de savoir a qui sont destinés les transferts de crypto-monnaies. C'est donc l'exigence de KYC pour *know your customer* qui semble souffrir d'une certaine aporie dans son application aux prestataires de service sur actifs virtuels.

B. L' apport du GAFI dans l'adaptation effective des dispositifs de lutte contre les nouvelles formes de criminalité

202.- Au-delà des constats qu'il réalise sur la base de son analyse des risques, le groupe d'action financière intervient aussi et surtout dans une démarche performative par l'émission de propositions concrètes. Bien que dénuées de force contraignante à l'instar des autres sources de la soft law[333], ces recommandations et lignes directrices n'en sont pas moins des instruments décisifs dans l'adaptation des États à leur environnement criminogène[334]. Elles offrent des voies d'amélioration des dispositifs nationaux en puisant dans les apports des différentes législations.

203.- La blockchain est abordée par le GAFI par le prisme des crypto-monnaies, laquelle est elle-même appréhendée au travers des prestataires sur actifs virtuels. C'est donc par le contrôle de ces intermédiaires que se focalise l'institution financière. S'il s'agit d'une étape nécessaire, cet encadrement n'est pas suffisant. Il laisse en effet de côté les transactions qui, nombreuses, s'opèrent en dehors de ces plateformes.

---

[331] Ibid, page 39.
[332] Ibid, page 282.
[333] Selon dictionnaire du droit international publié sous la direction de Jean SALOMON, la soft law désigne "*des règles dont la valeur normative serait limitée soit parce que les instruments qui les contiennent ne seraient pas juridiquement obligatoires, soit parce que les dispositions en cause, bien que figurant dans un instrument contraignant, ne créeraient pas d'obligation de droit positif, ou ne créeraient que des obligations peu contraignantes"* cité dans J.CAZALA, "Le *Soft Law* international entre inspiration et aspiration ». *Revue interdisciplinaire d'études juridiques*, 66, 41-84.
[334] Ibid, "*il existe un jeu d'influence du soft law sur les auteurs du hard law ou sur les énoncés hard law eux-mêmes"*.

204.- Approche par les risques[335]. Avant même de faire état de mesures pratiques, le GAFI souligne la nécessité pour les États d'adopter une position sceptique vis-à-vis des crypto-monnaies. Dénommée approche par les risques, cette exigence signifie que les transactions réalisées par ou en échange de ces actifs sont par nature suspectes - en raison de leurs caractéristiques déjà énoncées[336].

205.- Amplifier la connaissance des utilisateurs de PSAV. L'obligation KYC est une constante des normes LCB-FT. Consistant en un processus d'identification et de vérification de l'identité d'un client dans lequel une série de contrôles et de vérifications sont appliqués pour éviter les relations commerciales avec des personnes liées au terrorisme, à la corruption ou au blanchiment de capitaux[337], il s'agit pour les entités assujetties de vérifier avant toute transaction l'identité effective des opérateurs. En cas de suspicion sur l'intégrité des utilisateurs, elle permet d'activer l'obligation corrélative de déclaration de soupçon auprès des services de renseignement financiers, à l'instar de TRACFIN[338] en FRANCE. Pour l'heure, ces obligations - qu'il est possible de regrouper au sein d'une obligation générale de vigilance - sont circonscrites à certains seuils de déclenchement - en principe plus de 1000 euros pour une transaction - et concernent les clients habituels. S'agissant des PSAV, le GAFI précise que eu égard aux risques inhérents qu'ils suscitent, *"les pays peuvent (...) aller au-delà des exigences de la Recommandation 10 en imposant l'obligation de vigilance vis-à-vis de la clientèle pour toutes les transactions impliquant des AV ou réalisées par des PSAV (ainsi que d'autres entités assujetties, telles les banques qui s'engagent dans des activités d'AV), y compris les « transactions occasionnelles » au-dessous du seuil de 1 000 USD/EUR, conformément à leurs cadres juridiques nationaux[339]"*. Il s'agit ainsi de prévoir un abaissement du seuil d'activation de l'obligation de vigilance lorsque des intermédiaires sur crypto-monnaies sont concernés.

206.- L'usage de la blockchain pourrait s'avérer pertinent afin de remplir cette obligation. Pour pouvoir identifier les risques liés à un profil particulier, il faut d'abord collecter et centraliser les informations le concernant. Or, de par sa nature de registre sécurisé et public, la blockchain revêt les qualités requises pour en être le support. En ce sens, le GAFI propose notamment la création

[335] FATF (2019), Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers,
[336] Voir n° 181.
[337] https://www.electronicid.eu/fr/blog/post/kyc-know-your-customer-france/fr
[338] C. mon.fin., art, L. 561-15 : *" Les personnes mentionnées à l'article L. 561-2 sont tenues, dans les conditions fixées par le présent chapitre, de déclarer au service mentionné à l'article L. 561-23 les sommes inscrites dans leurs livres ou les opérations portant sur des sommes dont elles savent, soupçonnent ou ont de bonnes raisons de soupçonner qu'elles proviennent d'une infraction passible d'une peine privative de liberté supérieure à un an ou sont liées au financement du terrorisme"*.
[339] GAFI (2019), Lignes directrices de l'approche fondée sur les risques appliquée aux actifs virtuels et aux prestataires de services liés aux actifs virtuels

d'une blockchain dédiée à cet effet[340]. Pourraient être ainsi enregistrés les actifs les plus utilisés dans le cadre du blanchiment ou du financement du terrorisme - tel que Monero - afin d'éveiller la vigilance des PSAV ; les pays préalablement identifiés comme étant à risque par le GAFI ; les personnes physiques ou morales déjà connues pour des faits analogues ou similaires etc. Néanmoins, nonobstant l'existence de ce registre, la question de l'anonymat des transactions ne sera pas réglée. Il sera toujours possible pour les personnes identifiées d'adopter un pseudonyme et ne pas être détectées par les prestataires. C'est pourquoi de nouvelles techniques sont nécessaires.

207.- L'avènement d'une blockchain mondiale. Au-delà de cette utilisation comme instrument de conservation des données, la technologie de la chaîne de blocs pourrait, selon le groupe d'action financière, servir à des fins répressives ou à tout le moins d'enquête. En effet, *"les informations disponibles sur la chaîne de blocs (blockchain) ou l'autre type de registre distribué peuvent permettre aux autorités concernées de retracer les transactions jusqu'à une adresse de portefeuille[341]"*. Dès lors, en effectuant un transfert de bitcoins notamment, les plateformes peuvent suivre la destination de cet actif. En obtenant l'adresse publique de cet actif, l'auteur de la transaction a accès à tous les transferts dont il a fait et fera l'objet. Ainsi, il serait possible de remonter jusqu'à son bénéficiaire effectif, ce qui renforcerait l'efficacité du devoir de vigilance dans son volet connaissance des clients. La limite relative à l'utilisation d'adresses publiques et non de l'identité réelle des clients pourrait être équilibrée par la possibilité de procéder par recoupement des échanges effectués par une même adresse afin de remonter jusqu'à leur auteur[342]. Dans le cadre de l'action internationale de lutte contre la criminalité financière, la centralisation des informations au sein d'une blockchain partagée entre les différents services d'enquête des États membres offrirait une réponse globale et sans solution de continuité face à ce phénomène extraterritorial.

[340] Ibid, recommandation n° 11.
[341] Ibid.
[342] C'est de cette façon que les services d'enquête américains ont réussi en 2019 à identifier et arrêter le créateur d'un site pédopornographique présent sur le Darknet et permettant l'achat de contenu sexuel au moyen de bitcoins. Pour ce faire, ils ont envoyé une petite quantité de cette crypto-monnaie vers le portefeuille dédié à cet effet par le site. Dès lors, ils ont pu en suivre le cheminement jusqu'à aboutir au portefeuille du fondateur - un Sud-Coréen de 23.

Section 2. La mise en place d'une réponse opérationnelle effective

208.- Après avoir envisagé l'influence du GAFI sur la législation des États dans le cadre de la blockchain, il apparaît pertinent de s'interroger sur l'action effective - tant préventive que répressive - de ces derniers au niveau international. Il résulte en effet des enjeux soulevés par cette technologie que la lutte coordonnée des acteurs étatiques est une donnée centrale pour en limiter les risques. Comme évoqué précédemment, elle ouvre aux organisations l'accès à une criminalité sans frontières et par extension sans limites. Partant, l'internationalisation de la lutte doit être au cœur des efforts.

209.- L'action solidaire des États est la première branche de cette dynamique. Par solidaire il faut entendre, *"l'expression d'un esprit d'unité entre les individus, les peuples, les États et les organisations internationales, englobant la communauté d'intérêts, d'objectifs et d'actions et la reconnaissance de droits et besoins différents pour atteindre des objectifs communs*[343]*"*. Elle implique une action groupée et coalisée permettant la mise en commun de moyens matériels et humains. Pour ce faire, l'existence d'une instance transcendante est requise pour que se concrétise cette coopération opérationnelle. Or, sur la scène internationale, l'organisation Interpol fait office de modèle de référence dans la lutte contre la criminalité transfrontalière (**Paragraphe 1**).

210.- L'action conjointe quant à elle s'entend de l'effort partagé par les États à l'échelle nationale s'inscrivant dans le cadre international. Il s'agit donc ici d'initiatives étatiques mais prises en coordination avec les autres pays partenaires. Cette seconde conception de la lutte est dès lors au premier chef menée par un État, lequel peut faire appel au soutien d'un ou plusieurs de ses alliés par une demande d'entraide internationale (**Paragraphe 2**).

[343] *Projet de déclaration sur le droit à la solidarité internationale,* Haut conseil des droits de l'Homme de l'ONU, 25 avril 2017 et 19 juillet 2017, article 1er.

Paragraphe 1. Interpol, bras armé de la lutte internationale contre la criminalité 3.0

211.- Interpol est avant tout un réseau[344]. Ainsi, son office s'articule autour de celle des États qui la composent. Mais il s'agit aussi d'une organisation indépendante dotée de moyens propres[345], d'une structure précise[346] et d'équipes d'agents dédiés. Par conséquent, elle dispose d'une faculté de projection opérationnelle qui lui permet de répondre à des phénomènes criminels particuliers et identifiés comme relevant de la sphère internationale. Cette dualité en fait une structure hybride destinée à la fois à appuyer les États par le biais d'une contribution informationnelle (A) mais également au travers son action opérationnelle (B).

A. La contribution informationnelle d'Interpol

212.- L'organisation internationale de police criminelle - OIPC - Interpol dispose d'une expertise avérée en matière d'innovation et d'analyse criminelle. Sa composition diversifiée - agents des forces de sécurité, ingénieurs, juristes etc. - lui permet d'être en première ligne dans l'adaptation aux nouvelles formes de criminalité. Celle que permet la blockchain ne déroge pas à la règle. En effet, érigée en priorité par son secrétaire général Jürgen STOCK en octobre 2022, la prise en compte de la menace représentée par cette technologie et plus particulièrement par les crypto-monnaies, est désormais initiée. Elle passe tant par la formation des agents (1) que par le suivi des phénomènes criminels au profit des États (2).

1. Repenser la formation des forces de l'ordre

213.- L'une des missions fondamentales de l'organisation est la formation des agents étrangers. En effet, elle est désireuse d'assurer une réponse adéquate et un "renforcement des capacités". Pour ce faire, elle dispose de deux académies, l'Académie virtuelle[347] et l'Académie

[344] Comme le montre la présentation d'Interpol sur son site internet, il s'agit d'une instance regroupant 195 États qu'elle met en relation, voir https://www.interpol.int/fr/Qui-nous-sommes/Financement.
[345] Ibid, 137 millions d'euros de recette en 2021.
[346] Elle se compose d'un Secrétariat général dirigé par un Secrétaire général, d'une Assemblée générale, d'une Comité exécutif avec son président, de Bureaux centraux nationaux au sein de chaque États.
[347] Il s'agit de la plateforme d'apprentissage numérique d'Interpol.

mondiale d'Interpol[348], qui assurent une formation continue et régulière. Les différentes utilisations criminelles de la blockchain sont naturellement incluses dans les modules les plus récents. Mais au-delà de cette adaptation du contenu, une modernisation de la forme est possible. Pour s'adapter aux défis soulevés par la blockchain, Interpol a pu en exploiter les potentialités. En effet, lors de sa 90ème Assemblée générale à New Delhi, elle a annoncé le lancement de son propre métavers afin d'offrir aux enquêteurs une formation complète et immersive. Il s'agira donc de leur permettre d'interagir avec un environnement réaliste et ainsi d'être confrontés à des situations proches de celles qu'ils auront à connaître dans leur fonction.

2. Identifier les phénomènes criminels et permettre leur répression

214.- Connaître un phénomène criminel requiert parfois du temps. Or, dans un monde en constante accélération[349], la réponse se doit d'être immédiate. S'il est des technologies qui évoluent rapidement, c'est bien celles liées à la blockchain[350]. De nouvelles utilisations naissent régulièrement et sont autant de nouveaux risques en matière de sécurité. C'est dans ce contexte qu'Interpol peut déployer son expertise. L'organisation possède une connaissance fine et actualisée des nouvelles formes de criminalité qu'elle entretient par des cycles d'études thématiques. Récemment, la "Quatrième Conférence mondiale sur les fonds d'origine illicite et l'utilisation des cybermonnaies à des fins illicites" a été organisée par Interpol, Europol et l'Institut de Bâle sur la gouvernance[351] afin de développer des *"solutions intersectorielles à l'échelle internationale pour lutter contre l'utilisation des cybermonnaies à des fins criminelles[352]"*. Elle a notamment pour objet de *"renforcer les connaissances, l'expertise et les meilleures pratiques en matière d'enquêtes financières et de renseignement sur les actifs virtuels et les cybermonnaies"*. Par la mise en place d'une doctrine commune, les pays membres et leurs partenaires seront en mesure de répondre efficacement à cette criminalité 3.0.

215. - Centraliser l'information est l'autre mission clé d'Interpol dans le cadre de la coopération informationnelle. Regroupant dix-neuf bases de données différentes[353], accessibles à toutes les

[348] Il s'agit des formations dispensées au niveau régional par les partenaires d'Interpol.
[349] *Accélération*, H. ROSA, 2013.
[350]Selon le site Ledger.com, la blockchain serait actuellement dans sa troisième génération laquelle repose essentiellement sur l'interopérabilité.
[351] "Élaborer la réponse internationale à apporter à la criminalité financière et à l'utilisation des cybermonnaies à des fins illicites", Interpol, 20 novembre 2020.
[352] Ibid.
[353] Relative notamment aux personnes faisant l'objet d'une notice rouge - concernant les personnes recherchées par Interpol et devant faire l'objet d'une arrestation - les empreintes, les armes, les documents administratifs etc.

forces de l'ordre étatiques, l'Office est une source de référence pour lutter contre les groupes criminels de dimension internationale. Or serait-il possible d'automatiser la recherche des criminels ou des biens identifiés par Interpol ? La blockchain pourrait apporter une réponse affirmative. En utilisant la technologie des smarts contracts et en les configurant pour qu'ils mettent en relation les données enregistrées, la création d'une grande blockchain Interpol permettrait d'accroître l'identification des profils, notamment ceux des personnes placées sur notice rouge. Il s'agirait de recouper toutes les informations concernant un individu pour établir des liens entre différentes catégories de données. L'avantage par rapport au système actuel et qu'il s'agirait d'un registre unique et automatisé.

B. L'action opérationnelle d'Interpol

216.- Malgré leur adhésion à l'Organisation, les États ne se sont pas dépossédés de leurs prérogatives régaliennes en matière d'investigation et de poursuite pénales. Bien au contraire, cette institution constitue plutôt un catalyseur de leurs actions respectives en permettant leur inscription dans une démarche collective. En effet, si *"dans le passé, le rôle d'Interpol a trop souvent été perçu comme limité aux seuls échanges de renseignements policiers(...) il est aujourd'hui un acteur de premier plan en matière de sécurité ; il couvre tout le champ de l'action policière*[354]*"*.

217.- Pour pouvoir agir de concert, les équipes d'enquêteurs des différents États doivent communiquer en temps réel et sans difficultés liées à la langue. Cela nécessite en temps normal une préparation très en amont des opérations et de lourdes démarches. Mais ces nécessités chronophages ne sont pas solubles dans la criminalité liée à la blockchain. Une prompte réaction doit être opposée à ces faits occultes et déterritorialisés. C'est dans cette configuration qu'Interpol offre toutes ses potentialités. Au travers de son système de communication global et sécurisé appelé I-24 / 7, il assure une connexion entre les 195 pays membres. Ces derniers peuvent échanger via des canaux dédiés sur l'évolution d'une enquête et suivre en temps réel les avancées réalisées à l'étranger. Il s'agit du plus grand réseau policier mondial, largement dimensionné face à l'ampleur de la technologie de la chaîne de blocs

[354]R.NOBLE, L'Interpol du xxie siècle. *Pouvoirs* 132 , p. 103-116, 2010.

218.- Les actions communes entre plusieurs États sont une autre dimension de l'action opérationnelle d'Interpol. Grâce à son centre de commandement et de coordination, qui relie le Secrétariat général aux bureaux centraux nationaux et aux bureaux régionaux, il constitue une instance de surveillance disponible 24 heures sur 24 et accessible dans l'une des quatre langues officielles de l'organisation que sont l'anglais, le français, l'arabe et l'espagnol. C'est également cette cellule qui assure l'émission et la diffusion des notices - dont la plus connues et la notice rouge propre aux fugitifs - à la demande des États. A titre d'exemple, Interpol a émis une notice rouge contre Do Kwon, le créateur des crypto-monnaies Terra et Luna[355], après que le mandat d'arrêt émis par la Corée du Sud fut demeuré sans effet. Par la diffusion de cette notice, il n'y a maintenant presque aucun pays où il puisse se sentir en sécurité.

Paragraphe 2. L'action internationale des États dans la lutte contre la criminalité 3.0.

219. - Face à cybercriminalité liée à la blockchain, *"les règles du jeu international et les modèles stratégiques existants semblent inadaptés et surtout la vitesse des évolutions technologiques et opérationnelles dépasse celle de l'élaboration d'un consensus international et d'un nouveau corpus juridique[356]"*. Par conséquent, il a été démontré que le rôle d'institutions coordinatrices comme Interpol[357] pouvait s'avérer essentiel pour améliorer la lutte contre ces infractions complexes. Mais en dehors de ce cadre commun, il est également nécessaire que les États poursuivent leurs activités répressives. Confrontés à de nouveaux acteurs mieux adaptés à ces technologies innovantes, ils sont confrontés à une obligation de moyen, sinon de résultat. Or, force est de constater que, initialement, *"les États sont pris de court. Seuls quelques-uns d'entre eux avaient anticipé son importance future[358]"*.

---

[355] *Do Kwon est recherché pour son implication dans l'écosystème de crypto-monnaie Terra. Il s'agissait d'un projet de stablecoin algorithmique, qui était indexé sur le dollar et qui garantissait le prix de la crypto grâce à un système mathématique. La crypto-monnaie a par la suite perdu toute valeur, entraînant la perte de plus de 60 milliards de dollars. Terra a également emporté avec elle le très puissant fonds d'investissement Three Arrows Capital, qui a déclaré faillite. Bien que Do Kwon ait tenté de relancer un projet similaire pour éponger les pertes accumulées, ce dernier n'a jamais décollé et n'a jamais permis de dégager de l'argent"* cité depuis "Do Kwon, le fondateur de la crypto Terra, est maintenant un « fugitif » recherché par Interpol", Numerama, 26 septembre 2022, consulté le 12 décembre 2022.

[356] F. DOUZET. « La géopolitique pour comprendre le cyberespace ». In Hérodote 152-153.1 [2014], p. 3-21, p. 9.

[357] Voir n° 216 et suivants.

[358] L. PROSPERI, "Le cyber, un facteur d'instabilité internationale", https://laurentprosperi.info/fr/, 2020.

220.- La coopération pénale internationale se fonde sur l'idée selon laquelle à l'internationalisation de la criminalité doit répondre une globalisation de la répression. Tel est particulièrement le cas en matière de cybercriminalité. C'est ainsi que divers mécanismes ont été créés pour permettre aux États d'agir ensemble pour endiguer certains phénomènes identifiés tels que le trafic de stupéfiants[359], le crime organisé[360] ou encore le financement du terrorisme[361]. Or, tous ces instruments ont pour point commun d'instaurer des dispositifs d'entraide pénale internationale, entendue comme *"l'ensemble des moyens par lesquels une autorité étatique, dite autorité requise, prête le concours de sa force publique ou de ses institutions judiciaires à l'instruction, au jugement ou à la répression d'une infraction par une autre autorité judiciaire, dite autorité requérante[362]".* Ne dérogeant pas à cette loi d'airain de la lutte internationale, la criminalité 3.0 devra être appréhendée par le prisme de l'entraide pénale internationale avec ce qu'elle recèle de forces mais surtout de faiblesses (A).

221.- L'existence de cadres de coopération internationale plus étroits offre une réponse plus effective aux activités criminelles transnationales. Qu'il s'agisse d'accords bilatéraux ou multilatéraux, ils permettent aux États d'obtenir de leurs partenaires un soutien opérationnel plus rapide et harmonisé. Dans le cadre de la cybercriminalité - catégorie générique d'infractions à laquelle appartiennent celles commises par et contre la blockchain - c'est sous l'égide du Conseil de l'Europe[363] que se manifeste cette coopération renforcée et dont il s'agira d'analyser les potentialités face à cette criminalité (B).

---

[359] Convention des Nations Unies contre le trafic illicite de stupéfiants et de substances psychotropes, 1988

[360] Convention des Nations Unies contre le crime organisé, 2000.

[361] Convention internationale pour la répression du financement du terrorisme, 1999.

[362] C. LOMBOIS, Droit pénal international, 2e éd., 1979, *Dalloz*, in B. AUBERT, *"Entraide judiciaire : matière pénale", Répértoire de droit international,* Dalloz*,* 2005.

[363] Selon le site Viepublique.fr: *"Le Conseil de l'Europe est une organisation intergouvernementale. Il regroupe aujourd'hui 46 États dont les 27 États membres de l'Union européenne (UE). Il représente plus de 800 millions d'Européens".*

A. Forces et faiblesses de l'entraide pénale internationale

222.- Dans un ouvrage de référence[364]Henri DONNEDIEU DE VABRES distinguait trois formes d'entraide pénale[365] : celle relative à la documentation internationale - c'est-à-dire la communication de fichiers, casiers judiciaires ou bulletins - celle relative à la recherche et la poursuite des malfaiteurs et celle relative à l'assistance judiciaire - par le biais notamment des commissions rogatoires internationales, des actions policières coordonnées et des communications de pièces. C'est cette troisième hypothèse qui sera envisagée ici dès lors que les deux premières conceptions sont essentiellement ciblées sur des individus plus que sur l'acte en lui-même. Or, la criminalité 3.0 atténuant la possibilité de l'identification d'un auteur précis et se commettant en général dans le cadre d'organisations criminelles, il est nécessaire de l'appréhender directement.

223.- La réalisation d'actes de procédure à l'étranger est une étape fondamentale à la résolution d'affaires de nature internationale. Elle permet de poursuivre les investigations sans discontinuer et de déceler les éventuelles ramifications dissimulées à l'étranger. Il peut s'agir d'une demande d'extradition[366], d'une commission rogatoire internationale[367] ou encore d'une demande de saisie d'objets de nature infractionnelle. Quoi qu'il en soit, et dans le cadre international traditionnel, une telle demande s'effectue généralement en quatre temps[368].

224.- La formulation de la demande est le fait de l'autorité judiciaire désignée par le pays d'origine. En France, il s'agit en général des magistrats des juridictions répressives en ce compris les magistrats du parquet. La question du statut du procureur de la République ne fait donc ici pas difficulté dès lors que la demande sera soumise au filtre de l'autorité diplomatique.

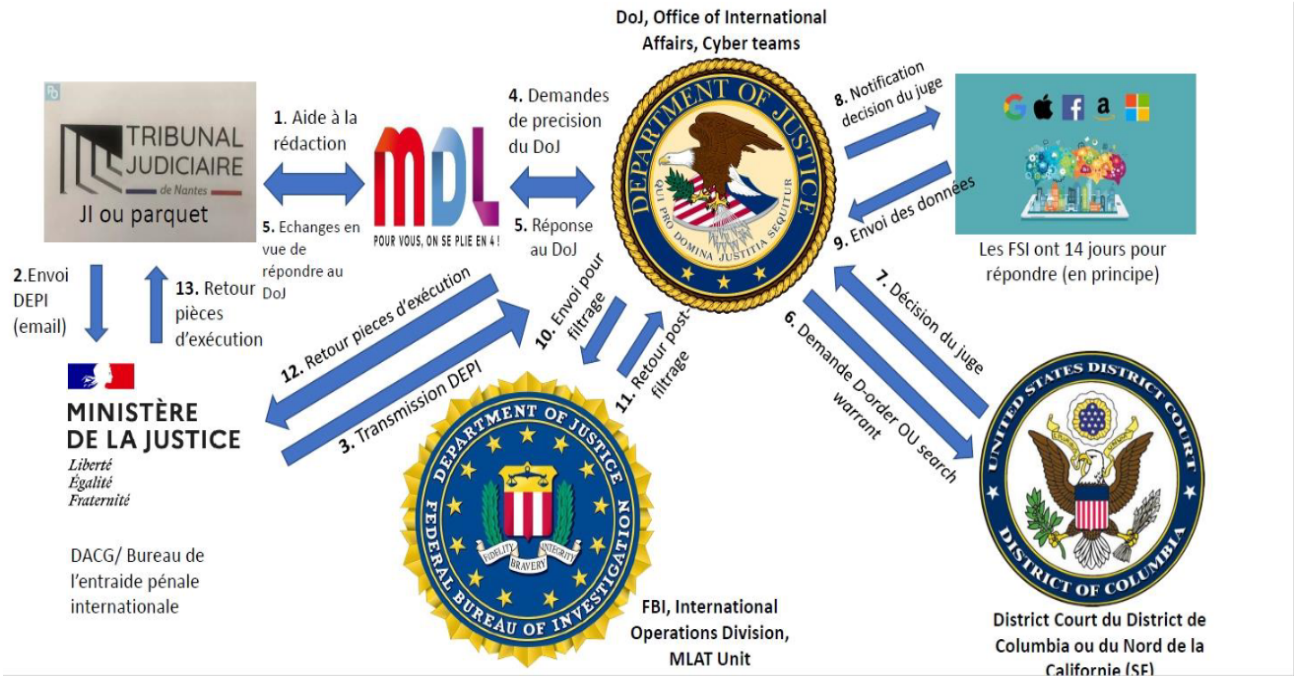
225.- La transmission de l'acte à l'État requis prend généralement la forme de la voie diplomatique. Un véritable parcours du combattant se met alors en branle : parquet compétent, Chancellerie, ministère des Affaires étrangères français, ministère des Affaires étrangères de l'État

---

[364] H. DONNEDIEU DE VABRES, *Les principes modernes du droit pénal international*, 1928, Sirey, p. 220 et s
[365]Op.cit, B. AUBERT, *"Entraide judiciaire: matière pénale"*.
[366] *"Mécanisme juridique par lequel un Etat (Etat requis) livre une personne qui se trouve sur son territoire à un autre Etat (Etat requérant) qui la réclame aux fins de poursuite ou d'exécution d'une peine",* A-M A ROSA, *Extradition* In : *Dictionnaire de droit international pénal : Termes choisis* [en ligne]. Genève: Graduate Institute Publications, 1998 (généré le 31 janvier 2023).
[367] *"Mission donnée par un juge à toute autorité judiciaire relevant d'un autre Etat de procéder en son nom à des mesures d'instruction ou à d'autres actes judiciaires"*, "Commission rogatoire internationales", *France diplomatie*, ministère des Affaires étrangères.
[368] Op. cit, B. AUBERT.

requis, ministère de la Justice de ce pays et enfin autorité compétente pour réaliser cet acte[369]". Durant ce délai, le produit de l'infraction - par exemple la rançon obtenue d'une cyberattaque et payée en bitcoins - aura pu être mélangé à d'autre crypto-monnaies, investi dans des NFT ou dans le Métavers puis converti en monnaie légale afin d'être réinjecté dans l'économie réelle.

226.- L'examen de la demande est également une étape caractérisée par sa lenteur. Si par principe ce contrôle est "modéré[370]", l'État requis se bornant à vérifier sa compétence et le respect de son ordre public, la coopération avec certains pays peut s'avérer beaucoup plus exigeante. Le cas des États-Unis est révélateur. Pour simplifier la présentation, il sera recouru à un schéma extrait du cours dispensé par Monsieur Xavier LEONETTI aux étudiants de master sécurité intérieure et à ceux du master lutte contre la criminalité financière et organisée.



Cheminement d'une demande d'entraide pénale internationale envoyée aux autorités américaines.

Comme le montre cette image, l'accumulation de services différents dans le pays requis provoque une embolisation de la procédure.

227.- L'exécution de l'acte par l'État requis enfin constitue l'achèvement de la procédure. Elle est réalisée conformément au droit du pays saisi. Or, s'agissant de la blockchain, ce principe de territorialité peut créer des difficultés lorsque l'État ne la reconnait pas et refuse par conséquent

[369] Ministère de la Justice, Définition des modes de transmission, "Voie diplomatique", .
[370] Op,cit, C. LOMBOIS.

d'en faire un objet susceptible d'investigations. Au surplus, il peut refuser d'accomplir la demande s'il estime que des motifs limitativement énumérés par les Conventions y font obstacle, ces motifs étant au demeurant très nombreux.

228.- L'efficacité de l'entraide pénale classique semble donc relative. Elle souffre des lourdeurs procédurales et d'une lenteur concomitante. De plus, la grande marge de manœuvre laissée aux pays requis rend parfois hypothétique leur réponse à une sollicitation concernant une matière aussi sensible que celle de la blockchain. Cette carence est renforcée par l'exigence du critère de réciprocité ou double incrimination des infractions qui est difficilement rempli en matière de cybercriminalité. Or*, "de nombreuses cyber infractions restent actuellement exclues de toute incrimination dans de nombreux États, rendant ainsi la commission rogatoire inopérante dans de nombreux cas. Cette différence des règles nationales applicables peut compromettre l'instruction des infractions transnationales, ce qui permet aux cybercriminels de continuer à échapper à la justice*[371]*"*.

229.- Pourtant, lorsque cette coopération fonctionne, elle est redoutable pour les criminels comme le rappelle l'exemple de l'affaire Liberty Reserve. Cette entreprise était une plateforme de transfert international de fonds. Pour procéder à une transaction, le client devait au préalable passer par un "changeur" afin que ce dernier convertisse l'apport en argent en une monnaie virtuelle appelée la Liberty Reserve et le conserve pour le client sur un compte dédié[372]. Bien que neutre dans sa conception, cette technique de conversion a été détournée à des fins de blanchiment de capitaux. Lorsqu'elle fut démantelée en 2013, l'entreprise avait permis la réalisation de 55 millions de transactions et le blanchiment de près de 6 milliards de dollars[373]. Ces fonds provenaient de fraudes par cartes de crédit, d'usurpations d'identité, de fraudes à l'investissement, de piratages informatiques, de la pédopornographie, de trafics de stupéfiants et d'autres crimes[374].

230.- Outre l'importance des intérêts financiers en jeu, c'est par l'ampleur de la procédure que cette affaire fait référence. En effet, de par son caractère international - le siège social se trouvait au

[371]S.JOISSAINS et J. BIGOT, *Cybercriminalité : un défi à relever aux niveaux national et européen,* Rapport d'information du Sénat fait au nom de la commission des affaires européennes et de la commission des lois, déposé le 9 juillet 2020.

[372] F. FABIANI, "Monnaie électronique et affaire Liberty Reserve : quelle réglementation applicable en France ?", Village justice, 13 juin 2013, consulté le 13 janvier 2023.

[373] *US v Liberty Reserve et al.,* Office des Nations Unies contre la drogue et le crime, "résumé des faits",

[374] "Chief Technology Officer of Liberty Reserve Sentenced to Five Years in Prison", *Department of Justice* , 12 décembre 2014.

Costa Rica mais les fonds étaient d'origines multiples - ce sont dix-sept pays qui furent concernés et huit services d'enquête différents ainsi qu'Interpol qui furent mobilisés. Or, pour réussir à appréhender ces infractions occultes, une coopération internationale efficace a dû être mise en place. Concrètement, celle-ci s'est fondée sur une initiative des autorités de poursuite costaricaines qui ont constaté un défaut de licence de l'entreprise pour exercer son activité d'intermédiaire financier et l'ont fait fermer. Par la suite, c'est le profil de son fondateur - Arthur BUDOVSKY - qui a alerté les autorités américaines lesquelles ont sollicité le Costa Rica pour qu'il engage une enquête[375]. Cette demande - commission rogatoire internationale - a permis la réalisation de perquisitions et de saisies dans les locaux de sociétés fictives et de résidences du suspect. In fine, c'est en Espagne que le fugitif a été retrouvé et renvoyé aux États-Unis à la suite d'une demande d'extradition. Dès le début de l'enquête internationale, le site Liberty Reserve a été fermé à titre conservatoire. Cela a permis de faire cesser l'activité criminelle durant la procédure qui a abouti après quatre ans. Commentant l'affaire, le procureur général de Manhattan a affirmé que *"comme la criminalité se mondialise de plus en plus, le bras long de la loi doit être encore plus long, et dans ce cas, il a encerclé la terre[376]".*

B. Le renforcement de l'entraide pénale internationale par la Convention de Budapest du 23 novembre 2001

231.- Adoptée dans le cadre du Conseil de l'Europe, cette Convention a été ratifiée par 65 pays dont certains ne sont pas membres du Conseil comme les États-Unis, l'Australie ou encore le Japon[377]. Composée de quatre chapitres relatifs respectivement à la I) La terminologie; II) Les mesures à prendre au niveau national; III) La coopération internationale; IV) Les clauses finales, elle couvre de nombreux pans de la cybercriminalité en imposant des obligations renforcées en matière de coopération.

232.- Application à la blockchain. Parmi les infractions visées, la Convention fait notamment référence a "*toute forme d'atteinte au fonction d'un système informatique dans l'intention, frauduleuse ou délictueuse, d'obtenir sans droit un bénéfice économique pour soi-même ou pour*

[375] D. BODIGER et L. ARIAS, "Millions of dollars in limbo after shuttering of digital currency site Liberty Reserve", TicoTimes.net, 24 mai 2013, consulté le 12 janvier 2023.
[376] J. CLOTHERTY, "Black Market Bank' Accused of Laundering $6B in Criminal Proceeds", abc. news, 29 mai 2013, consulté le 12 janvier 2023.
[377] N. OUCHENE, *L'applicabilité de la loi pénale à l'endroit de la cybercriminalité dissimulée.* Droit. Université Paris 2 Panthéon-Assas, 2018.

autrui[378]*"*. Or, dans la mesure où la conception retenue de la blockchain est celle d'un système de traitement de données à caractère personnel[379], il est permis de lui étendre le champ matériel de la Convention de Budapest.

233.- Principe de coopération internationale renforcée. L'article 23 de la Convention stipule au titre des principes généraux relatifs à la coopération internationale que *"les Parties coopèrent les unes avec les autres, conformément aux dispositions du présent chapitre, en application des instruments internationaux pertinents sur la coopération internationale en matière pénale, des arrangements reposant sur des législations uniformes ou réciproques et de leur droit national, dans la mesure la plus large possible, aux fins d'investigations ou de procédures concernant les infractions pénales liées à des systèmes et des données informatiques ou pour recueillir les preuves, sous forme électronique, d'une infraction pénale*[380]*"*. Cette affirmation qui irrigue toute la philosophie de ce texte, offre aux États la certitude d'une entraide effective.

234.- A la source, l'information. Toute procédure pénale, qu'elle soit de nature interne et a fortiori de nature internationale, résulte d'une information. Celle-ci permet aux autorités de poursuite de mener une enquête préliminaire[381] voire de flagrance[382] si les éléments sont suffisamment étayés. Mais cette connaissance peut parfois être ralentie par les délais inhérents aux processus classiques de coopération reposant sur une demande préalable de l'État. La Convention permet de pallier en partie cette difficulté. Tout État membre peut en effet procéder à une communication spontanée d'information à l'un de ses partenaires s'il estime *"que cela pourrait aider la Partie destinataire à engager ou à mener à bien des enquêtes ou des procédures au sujet d'infractions pénales établies conformément à la présente Convention, ou lorsque ces informations pourraient aboutir à une demande de coopération formulée par cette Partie au titre du présent chapitre*[383]*"*. En ce qui concerne la blockchain, et notamment les infractions reposant sur des schémas de fraude récurrents - comme les investissements de type pyramide de Ponzi - l'information permettra de déceler et d'annihiler cette opération. Ainsi, il pourra être important de savoir si l'entreprise dans laquelle l'investissement doit être effectué existe et est le cas échéant enregistrée dans un pays membre.

[378] Ibid.
[379] Voir n°59.
[380] Article 23 de la Convention de Budapest, STCE 185, p 13.
[381] C.proc. pén., art. 75.
[382] C.proc. pén., art. 53.
[383] Article 26.

235.- Pour identifier, l'accès aux preuves. L'obtention de preuves constitue pour toute procédure pénale la composante cardinale. Car, *idem est non esse non probari*[384], les autorités de poursuite à qui incombent la charge de la preuve[385], doivent pouvoir démontrer avec assez de consistance que les faits ont bien été commis et le cas échéant l'imputer à un individu. Or, comment attribuer une infraction commise de manière anonyme sur la blockchain, et qui plus est commise depuis l'étranger, sans preuves ? La Convention de Budapest permet en partie de simplifier l'échange de preuves entre États sans pour autant en régler toutes les lacunes. En effet, aux termes de son article 32, une Partie peut, sans l'autorisation de l'autre, *"accéder à des données informatiques stockées accessibles au public (source ouverte), quelle que soit la localisation géographique de ces données"*. Est donc consacré l'accès aux données contenues sur un système informatique situé à l'étranger. Cela permet notamment aux enquêteurs de pouvoir agir rapidement aux fins d'obtenir des données concernant les individus ayant participé à une opération criminelle. Par exemple, il serait possible d'identifier les auteurs d'une infraction commise dans le Métavers en saisissant leurs identifiants de connexion et ce même s'ils sont connectés depuis l'étranger.

236.- Pour interpeller, agir en commun. La coopération internationale n'est jamais aussi efficace que lorsqu'elle passe par des actions opérationnelles communes. A cet égard, la Convention de Budapest s'est dotée d'un deuxième protocole additionnel[386]. Ce nouvel instrument prévoit notamment un article 12 relatif aux équipes communes d'enquête. Plus précisément, *"lorsqu'une coordination renforcée est considérée comme particulièrement utile, d'un commun accord, les autorités compétentes de deux ou plusieurs Parties peuvent établir et faire fonctionner une équipe commune d'enquête sur leurs territoires pour faciliter les enquêtes ou les poursuites"*. Ainsi, à l'instar de ce qui existe déjà dans le cadre restreint de l'Union européenne[387], les États ayant signé et ratifié le protocole additionnel pourront désormais établir de telles équipes afin de mener des investigations sur leurs territoires distincts. Il s'agira de permettre une accélération considérable de l'enquête et combattre la volatilité des crypto-monnaies avant qu'elles ne soient blanchies ou de saisir les ordinateurs des mineurs installés dans des pays en voie de développement comme ceux du Maghreb - partie à la Convention - et utilisés pour commettre des attaques contre la blockchain. Pourraient aussi être envisagées des équipes d'enquête dans le Métavers afin de suivre la trace des

[384]X LAGARDE, *La preuve en droit*. in Dominique Rousseau éd., *La Preuve* (pp. 101-124). Odile Jacob, 2003.
[385] C.civ., art. 1353: *"Celui qui réclame l'exécution d'une obligation doit la prouver"*.
[386] Approuvé par le Comité des ministres le 17 novembre 2021, il a été ouvert à la signature en mai 2022.
[387]Décision-cadre du Conseil du 13 juin 2002 relative aux équipes communes d'enquête

flux financiers illégaux ou des auteurs d'infraction où qu'ils se trouvent. Reste désormais à attendre que le plus grand nombre de pays adhèrent à ce protocole.

Conclusion du Chapitre 1

237.- Un rapprochement mesuré mais volontariste caractérise ainsi l'action répressive des États sur la scène internationale relativement à la criminalité blockchain. Celle-ci repose tant sur des mécanismes connus du droit pénal international - mais adapté aux particularismes de cette technologie - que sur des outils plus poussés de coopération. À cet égard, il est permis de remarquer que plus le cadre est restreint plus la lutte apparaît efficace - à tout le moins effective - face à des phénomènes nouveaux. Par conséquent, il semble que la meilleure réponse soit celle d'une prise en compte au niveau le plus fin de coopération pénale, cadre qu'offre l'Union européenne (**Chapitre II**).

Chapitre II. La coopération européenne renforcée comme substitut à l'action unique de l'Union européenne

238.- Une approche pragmatique face aux nouveaux défis. *"L'Europe ne se fera pas d'un coup, ni dans une construction d'ensemble : elle se fera par des réalisations concrètes créant d'abord une solidarité de fait*[388]*".* Pour le ministre des Affaires étrangères d'alors, l'Union européenne - d'abord appelée Communauté européenne - devait être fondée sur la rationalité des dirigeants face aux risques de la guerre. Reposant d'abord sur la nécessité, cette entité *sui generis*[389] a peu à peu gagné en légitimité et en compétences. Dans le cadre de son troisième pilier "justice et affaires intérieures", des "domaines d'intérêt commun" sont énumérés[390] et notamment la coopération judiciaire en matière civile et pénale[391] ainsi qu'une coopération policière et douanière[392]. La

[388] R. SCHUMAN, "Déclaration du 9 mai 1950".
[389] S. HENRY, "L'Union européenne, une construction *sui generis"*. in S. Henry, *Droit de l'Union européenne*, Ellipses, 2020, p. 28 à 42.
[390] "Le troisième pilier de l'Union européenne: justice et affaires intérieures", CVCE,
[391] TFUE., art. 82: *"La coopération judiciaire en matière pénale dans l'Union est fondée sur le principe de recon naissance mutuelle des jugements et décisions judiciaires et inclut le rapprochement des dispositions législatives et réglementaires des États membres dans les domaines visés au paragraphe 2 et à l'article 83".*
[392] TFUE., art. 87: *"L'Union développe une coopération policière qui associe toutes les autorités compétentes des États membres, y compris les services de police, les services des douanes et autres services répressifs spécialisés dans les domaines de la prévention ou de la détection des infractions pénales et des enquêtes en la matière".*

suppression de cette organisation en piliers par le traité de Lisbonne[393] a renforcé la place des instances européennes dans le domaine répressif en facilitant les procédures d'adoption d'actes et en limitant corrélativement la place des États. En regard des menaces que font naître les utilisations criminelles de la blockchain et notamment leur dimension transfrontière, le cadre de l'Union européenne semble privilégié pour apporter une réponse forte et volontariste.

239.- Compétence des États ou compétence de l'Union ? Nonobstant cette extension du domaine d'intervention de l'UE, la politique pénale reste au premier chef l'apanage des États membres. En effet, "*l'Union européenne n'a pas vocation à élaborer un code pénal européen, les États membres restant souverains en la matière. Cependant, elle peut définir des lignes directrices et apporter une plus-value aux systèmes nationaux. Elle a surtout vocation à les aider à se coordonner*[394]*"*. Dès lors, c'est fondamentalement au niveau étatique que l'action pénale européenne tend à se déployer. Le champ de la cybercriminalité étant désormais une priorité au même titre que le trafic de stupéfiants ou le blanchiment de capitaux[395], l'appréhension de la criminalité liée à la technologie de la chaîne de blocs est a priori faite par les États sous l'égide de l'Union (**Section 1**).

Cependant et dans la mesure où l'Union européenne dispose de la capacité *"d'établir des règles minimales relatives à la définition des infractions pénales et des sanctions dans des domaines de criminalité particulièrement grave revêtant une dimension transfrontière résultant du caractère ou des incidences de ces infractions ou d'un besoin particulier de les combattre sur des bases communes dans les domaines de lutte contre le terrorisme, la traite des êtres humains et l'exploitation sexuelle des femmes et des enfants, le trafic illicite de drogues, le trafic illicite d'armes, le blanchiment d'argent, la corruption, la contrefaçon de moyens de paiement, la criminalité informatique et la criminalité organisée*[396]*",* il faut également mettre en exergue son rôle moteur dans la lutte contre cette criminalité (**Section 2**).

[393] Signé le 13 décembre 2007 et entré en vigueur le 1er décembre 2009.
[394] "La coopération judiciaire en matière pénale", Touteleurope.eu, 16 février 2018.
[395] Comme le montre l'adoption de nombreux instruments en la matière depuis la directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil (dite «directive cybercriminalité»)
[396] TFUE., art. 83.

Section 1. L'action des États sous l'égide de l'Union européenne

240.- Le principe de reconnaissance mutuelle au prisme de la lutte. Comme l'affirme l'article 82 du TFUE, *"la coopération judiciaire en matière pénale dans l'Union est fondée sur le principe de reconnaissance mutuelle"*. Cela signifie qu'aux modalités traditionnelles de coopération internationale, succèdent des processus simplifiés et renforcés d'action commune. Dans le champ du droit pénal lato sensu, cette "spécificité de l'Union européenne[397]" se manifeste par de nombreux dispositifs opérationnels auxquels participent les États membres (**Paragraphe 2**). Toutefois, afin d'être en situation de pouvoir agir en symbiose, il est au préalable nécessaire que les États disposent des informations suffisantes pour ajuster leur apport opérationnel. Cette première forme de coopération est de nature informationnelle (**Paragraphe 1**).

Paragraphe 1. La participation des États à la coopération informationnelle de l'Union

Plutôt que de négliger la blockchain, il serait possible de s'en servir à des fins utiles à la recherche d'informations (A) et ce malgré des limites inhérentes à son fonctionnement (B).

A. Une utilisation intelligente de la blockchain au service de l'information commune

241.- Si l'information est la clef de voûte de la procédure pénale nationale, *"son importance est accrue lorsque les faits infractionnels sont emprunts d'un élément d'extranéité[398]"*. Le cadre offert par l'Union européenne a ceci de particulier qu'il est à la fois un catalyseur des infractions transfrontières - facilitée par la libre circulation des personnes et des capitaux - mais également un vecteur de coopération policière et judiciaire efficace. Parmi les différents dispositifs qui permettent aux États de lutter ensemble contre cette criminalité a-étatique, l'échange d'informations est une prémisse essentielle de laquelle découle in fine l'identification des auteurs.

[397] I. JEGOUZO, "Le développement progressif du principe de reconnaissance mutuelle des décisions judiciaires pénales dans l'Union européenne", *Revue internationale de droit pénal*, 2006/1-2 (Vol. 77), p. 97-111.
[398] M. DUTHOIT, *La coopération pénale au sein de l'Union européenne,* Panthéon Assas, 2010.

242.- Les systèmes policiers et judiciaires de l'Union européenne sont suffisamment nombreux[399] pour couvrir quasiment tout le spectre des infractions. Malgré leur complétude, ces fichiers souffrent tous d'une aporie fonctionnelle liées à l'absence de centralisation. Chaque fichier est en effet alimenté par les États et met en réalité en commun les différents fichiers nationaux par un système de renvoi. A titre d'exemple, le système ECRIS recèle les possibilités mais surtout les limites de ce partage d'informations. Ce fichier des casiers judiciaires nationaux repose sur un procédé décentralisé. En cas de condamnation dans un État membre, ce dernier doit communiquer à l'État d'origine de l'individu les informations y afférentes afin qu'il les enregistre dans son système national. Si le même individu est de nouveau condamné ou fait l'objet d'une autre procédure pénale dans un autre État membre, ce dernier pourra alors consulter son casier judiciaire en passant par le fichier ECRIS qui lui-même renverra au fichier situé dans son État d'origine. Cette chaîne complexe de circulation de l'information, bien que souhaitable, n'est pas satisfaisante en matière de criminalité portant sur des crypto-monnaies, caractérisée par la rapidité de dissipation des fonds et des personnes. Les délais incompressibles que cette procédure impose ne sont pas compatibles.

243.- La blockchain pourrait ici être employée aux fins de simplification de l'accès à l'information[400]. Dans le cadre de son utilisation comme registre décentralisé, la technologie de la chaîne de blocs est parfois convoquée comme la panacée. En effet, en ce que l'information qui y est inscrite est enregistrable par tous et accessible à tous, il serait possible de concevoir une blockchain européenne centralisée - au niveau d'Europol par exemple - et au sein de laquelle seraient enregistrées toutes les informations concernant, outre l'identité des auteurs condamnés, celle des personnes recherchées, dangereuses, en fuite ou en attente d'une procédure d'extradition. Tout service préalablement autorisé à consulter cette blockchain - qui serait donc privée - pourrait accéder à une information immédiate, fiable car validée au préalable, actualisée par l'ajout de nouveaux blocs et inaltérable.

[399]Ils sont d'ailleurs si nombreux qu'ils ont fait l'objet d'une thèse consacrée précisément aux *Fichier pénaux de l'Union européenne* écrite par A. MORNET et à paraître en 2023.
[400] N. CATELAN, La blockchain au service du droit pénal « Colloque Blockchain et droit » Université de Brasilia, avril 2019 in Acheronta Movebo.

B. Les limites inhérentes au fonctionnement de la blockchain

244.- Des doutes sont émis quant à la faisabilité pratique d'une telle proposition[401]. En réponse à l'interrogation soulevé par la confrontation de cette technique d'identification au droit des personnes condamnées à la réhabilitation judiciaire par l'effacement du casier[402], qu'il soit permis d'opposer la nature particulière de cette blockchain telle que l'auteur de ce mémoire l'envisage. Il s'agirait d'une blockchain privée, c'est-à-dire, créée et gérée par une entité centrale institutionnalisée. Ce faisant, seul cet organe pourrait autoriser les services compétents pour consulter les données stockées. De plus, les paramètres de cette blockchain pourraient expressément prévoir - par le biais de smarts contracts - la suppression automatique des informations à l'issue du délai d'épreuve uniformisé. Enfin, il serait possible - sans qu'une attaque 51 % ne soit nécessaire - de modifier certains blocs pour y ajouter ou retirer des données dès lors que la validation reposerait non pas sur une preuve de travail mais sur une preuve d'autorité[403].

245.- Un encadrement nécessaire est donc la condition préalable à l'utilisation de cet outil. Il faudrait pour cela l'intégrer dans le cadre de l'action commune de l'Union européenne au sein d'un instrument existant - fichier SIS[404] , ECRIS ou ECRIS-TCN selon la nationalité du ressortissant - ou créer un instrument ad hoc. Pour cela, une vision communautaire de la blockchain est requise, ce qui implique une acception identique. A l'instar de l'échelon international, certains États de l'Union pourraient être rétifs à un tel engagement qui porterait atteinte à leur souveraineté pénale. En effet, la blockchain aboutissant à une décentralisation de la connaissance, le poids des États s'en trouve corrélativement amoindri. L'exemple de la Pologne ou de la Hongrie, dont les systèmes judiciaires sont les plus critiques, ne doit pas cacher les risques induits par les autres États membres.

---

[401] Ibid.

[402] C.pr. pén., art. 782: "toute personne condamnée par un tribunal français à une peine criminelle, correctionnelle ou contraventionnelle peut être réhabilitée".

[403] Ce système repose sur l'attribution du monopole de validation des transactions au sein des blocs à un utilisateur ou un groupe d'utilisateurs identifiés qui *"valident donc les transactions et les blocs et décident de ceux qu'il convient d'ajouter à la chaîne". DUMAS Jean-Guillaume, LAFOURCADE Pascal, TICHIT Ariane et al., « 6. Qu'est-ce qu'une preuve d'autorité ? », dans : , Les blockchains en 50 questions. Comprendre le fonctionnement de cette technologie,* sous la direction de J-G. DUMAS, P. LAFOURCADE, A. TICHIT et al. Paris, Dunod, « Hors collection », 2022, p. 23-25.

[404] Système d'identification Schengen.

Paragraphe 2. L'action opérationnelle des États dans le cadre coopératif d'Europol

A. Le rôle fondamental d'Europol en matière informationnelle

245.- Europol est l'agence européenne de coopération policière. Depuis sa création informelle au sein du groupe TREVI en 1975, la coopération des États membres de l'Union n'a cessé de se renforcer. D'abord limitée aux trafics internationaux de stupéfiants, elle a par la suite connu une extension de son domaine d'action[405]. Devenant progressivement un succédané de FBI européen[406], l'Office tend désormais à *"renforcer l'action des autorités compétentes des États membres et leur coopération mutuelle dans la prévention de la criminalité organisée, du terrorisme et d'autres formes graves de criminalité affectant deux États membres ou plus et dans la lutte contre ces phénomènes[407]"*.

246.- Centralisation des informations et mise en lumière des menaces émergentes. Telles sont les deux premières missions d'Europol. En effet, de par sa couverture territoriale étendue à tous ses membres par le biais d'officiers de liaisons, cette structure dispose d'une vision holistique de la criminalité. Elle observe les phénomènes criminels en croissance et les nouvelles méthodes employées par les auteurs d'infractions transfrontalières. La technologie blockchain constitue à ce titre l'apparition la plus récente. Dans son dernier rapport IOCTA[408] pour l'année 2021, l'Office soulignait notamment que le confinement avait accru de façon exponentielle les infractions commises en ligne. Étaient entre autres dénoncées les utilisations détournées de certains dispositifs à des fins criminelles. Les crypto-monnaies sont pointées du doigt, tant en ce qui concerne leur emploi comme moyen de paiement dans le cadre de ransomware que dans leur application aux fins

[405]P. GERBET, Europol, CVCE.ue.
[406] Europol est devenue une agence officielle de l'Union européenne depuis le 1er janvier 2010, "A propos d'Europol", Europol.europa.eu., 24 janvier 2023.
[407] RÈGLEMENT (UE) 2016/794 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 11 mai 2016 relatif à l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) et remplaçant et abrogeant les décisions du Conseil 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI et 2009/968/JAI.
[408] Les rapports IOCTA - Internet Organized Crime Threat Assessment - sont des publications annuelles au travers desquelles Europol met en lumière les menaces qu'elle a identifiées comme étant les plus préoccupantes.

de blanchiment d'argent, avec une augmentation notable de l'usage de Monero[409] sur le Darknet, ainsi que diverses fraudes ayant comme vecteur les crypto-monnaies[410].

B. Le rôle moteur d'Europol en matière opérationnelle

247.- Face à ces risques avérés, les États trouvent en Europol une organisation idoine pour faciliter la coopération de leurs forces de sécurité. Celle-ci permet tout d'abord l'établissement d'équipes communes d'enquête[411] destinées à étendre la poursuite et la répression des processus criminels - en particulier les blanchiments internationaux de capitaux - entre services répressifs de plusieurs États. A titre d'exemple, le 12 janvier 2023, Europol allié à Eurojust ainsi que les enquêteurs allemands, bulgares, chypriotes et serbes, a démantelé un système d'escroquerie internationale à la crypto-monnaie. Ce réseau criminel a incité des milliers de petits investisseurs à acheter des crypto-monnaies sur de faux sites en recourant à des centres d'appel disséminés sur plusieurs pays européens. Grâce à un travail coordonnés reposant notamment sur la réalisation de perquisitions simultanées dans les États d'origine des criminels, cette équipe commune a saisi trois portefeuilles matériels contenant environ 1 million de dollars de crypto-monnaies[412]. Sans une approche cohérente et une formation préalable des forces d'intervention, ces actifs auraient pu passer inaperçus. Cela souligne donc la nécessité, déjà préconisée par Interpol[413] dans ses sept recommandations en la matière, de la multidisciplinarité des équipes d'enquête ainsi que du partage technologique.

248.- La coopération au sein de l'Union européenne, qu'elle soit informationnelle - par l'échange d'informations ou l'alimentation des fichiers - ou opérationnelle - par la mise en place et l'animation d'équipes communes d'enquête - est particulièrement adaptée aux infractions facilitées par la blockchain. Elle en épouse à la fois la dimension transnationale en offrant une réponse analogue mais également la célérité et l'opacité par des moyens mutualisés et factorisés. Pour ne

[409] Plus précisément, le rapport souligne que bien que le bitcoin soit encore la monnaie virtuelle la plus usitée - y compris sur le Darkweb - sa conversion se fait bien souvent en Monero par le biais de "chain swapping". Cette tendance participe d'un mouvement plus général de complexification des méthodes de blanchiment qui reposent désormais sur des mélangeurs, des sauts de chaînes, des plateformes de conversion etc.
[410] Europol (2021), Internet Organised Crime Threat Assessment (IOCTA) 2021, Publications Office of the European Union, Luxembourg.
[411] Voir n°236 pour une définition.
[412] "Des réseaux de ventes de fausses crypto-monnaies démantelés en Bulgarie, en Serbie et à Chypre", Cybersécurité-solutions. com, 13 janvier 2023.
[413] "Recommendations of the 4th Global Conference on Cryptocurrencies and Criminal Finances" in *4th Global Conference on Cryptocurrencies and Criminal Finances* on 18-19 November 2020.

pas que des pays deviennent des espaces sans contrôle et des paradis artificiels[414] pour les criminels, le bras armé de l'Union doit pouvoir les frapper où qu'ils se situent - à tout le moins dans la limite de son emprise territoriale, ce qui pose des limites concrètes en une période où l'adhésion à cette institution se fait de plus en plus clivée.

Section 2. L'action de l'Union européenne transcendant celle des États

249.- En outre, et afin d'agir de concert au niveau national, ces derniers sont soumis à des obligations - qu'ils ont par définition librement acceptées - d'harmonisation de leurs législations avec celles de leurs partenaires européens, aiguillés en ce sens par les directives de l'Union (**Paragraphe 1**). Dans son état le plus abouti, l'action de l'Union européenne en matière de criminalité blockchain pourrait être incarnée au sein d'un organe judiciaire déjà existant : le parquet européen (**Paragraphe 2**).

Paragraphe 1. L'harmonisation des législations nationales, préalable à la cohérence de la lutte des États dans le cadre de l'Union européenne

En écho au développement de l'usage de la blockchain en général et des crypto-monnaies en particulier, deux voies sont permises sans s'exclure mutuellement. L'une consistant, de manière traditionnelle, à répondre aux défis criminogènes par une prévention et une répression à effet dissuasif. Il s'agit ici de l'approche la plus répandue au sein des États et c'est celle choisie par l'Union européenne (A). Dans une acception plus constructive, il est aussi possible d'opposer à une utilisation anarchique de la blockchain un usage encadré et contrôlé par la création d'une blockchain institutionnelle, sorte de monnaie européenne virtuelle dont les potentialités seraient tangibles (B).

[414] Que cette référence à Baudelaire nous soit permise.

A. Une première approche répressive

250.- L'Union européenne dispose de prérogatives en matière répressive afin de mettre les droits nationaux en conformité avec les orientations qu'elle s'est fixées. A cet égard, la Commission européenne joue un rôle prépondérant d'impulsion et de modernisation des instruments de prévention et de répression de la criminalité portant atteinte aux intérêts de l'Union. Parmi ces risques en lien avec la blockchain, le blanchiment de capitaux et le financement du terrorisme ont été identifiés comme étant les plus sensibles[415]. Dans ce contexte, c'est ce domaine qui a été le plus investi par les mesures d'harmonisation européennes.

251.- La lutte contre le blanchiment et le financement du terrorisme constitue, pour l'Union européenne, une priorité d'action inscrite dans la durée[416]. De plus, les directives dites "anti-blanchiment" de l'Union se caractérisent par leur adéquation avec les enjeux contemporains auxquels sont confrontés les États et auxquels elles répondent de manière circonstanciée. En ce qui concerne la blockchain et surtout les crypto-monnaies - que les directives qualifient d'actifs numériques - la 5ème directive[417] ne déroge pas à la règle. À la lecture de ce texte, il est permis d'en extraire les apports majeurs.

252.- Soumission des PSAN aux normes LCB-FT. Consciente des insuffisances dans la régulation des prestataires de service sur actifs numériques, la directive enjoint aux États membres de les assujettir de manière plus étroite aux normes issues des recommandations internationales comme celles du GAFI. C'est ce qui a été accompli en France par le biais de la loi PACTE précédemment évoquée[418]. Toutefois, le texte souligne immédiatement les limites de cet encadrement en ce que *"les utilisateurs peuvent également effectuer des transactions sans passer par de tels*

[415]Communication de la Commission relative à un plan d'action pour une politique globale de l'Union en matière de prévention du blanchiment de capitaux et du financement du terrorisme (doc. ST 7870/20), 7 mai 2020.

[416]C J. BERR, "Blanchiment de capitaux et financement du terrorisme", *Répertoire de droit commercial*, Dalloz, Janvier 2010 (actualisation : Octobre 2022) : *" C'est sur la base d'une convention élaborée au Conseil de l'Europe, le 8 novembre 1990, relative au blanchiment, au dépistage, à la saisie et à la confiscation des produits du crime, qu'a été arrêtée la directive nº 91/308/CEE du Conseil du 10 juin 1991, « relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux"*.

[417] Directive (UE) 2018/843 du Parlement européen et du Conseil du 30 mai 2018 modifiant la directive (UE) 2015/849 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme ainsi que les directives 2009/138/CE et 2013/36/UE

[418] Voir n°189.

prestataires[419]*"*. Pour pallier cette possibilité de contournement, il est notamment préconisé de renforcer le recours, par les services de renseignement nationaux, à la technique de traçage des transactions déjà évoquée ainsi et surtout que de permettre aux utilisateurs de procéder à des autodéclarations[420]. Cette dernière perspective à l'avantage de produire une information décentralisée et spontanée mais l'inconvénient de ne pas trouver à s'appliquer au cas de détournements de la blockchain à des fins criminelles. Enfin, la nature de ce texte - une directive qui impose aux États d'adopter des standards communs tout en les laissant libres de les adapter à leur cadre national - rend son efficacité relative. De plus, le texte ne s'applique qu'aux prestataires situés sur le territoire de l'Union européenne. Or, le risque est grand que les organisations criminelles décident de délocaliser leur activité de blanchiment dans des zones de non droit. Par conséquent l'adoption d'un acte plus contraignant paraît s'imposer.

253.- Vers une extension des contraintes en matière de crypto-monnaies ? Prenant acte des lacunes persistantes, les États ont arrêté par la voix du Conseil et du Parlement, une proposition de règlement et de directive en date du 7 décembre 2022. Ces deux textes sont destinés à renforcer le "corpus règlementaire de l'Union[421]" en matière de blanchiment de capitaux et financement du terrorisme. Ils prévoient notamment de soumettre les pays tiers aux obligations pesant déjà sur les prestataires situés sur le territoire de l'Union européenne afin de limiter les risques de "forum juridique". De son côté, Le 20 juillet 2021, *"la Commission a présenté un ensemble de propositions législatives visant à renforcer les règles de l'UE en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme*[422]*"* dont l'une tend à l'instauration d'une Agence européenne de lutte contre le blanchiment de capitaux. Cette institutionnalisation de la lutte européenne permettrait aux États d'agir au sein d'un cadre commun spécifique permettant une plus grande adaptation face aux nouveaux schémas de blanchiment utilisant la blockchain. Il faudra toutefois veiller à ce que cette nouvelle entité ne bouleverse pas le cadre actuel de coopération opérationnel déjà en vigueur.

[419]Directive (UE) 2018/843, paragraphe 9.
[420] Ibid.
[421] "Lutte contre le blanchiment de capitaux et le financement du terrorisme", Conseil européen.
[422] "Lutte contre le blanchiment de capitaux: le Conseil arrête sa position sur un corpus réglementaire renforcé", Conseil de l'UE, communiqué de presse, 7 décembre 2022.

B. La création d'un "crypteuro", solution envisageable pour lutter contre la criminalité 3.0

254.- Dans un rapport publié en octobre 2020, la Banque centrale européenne (BCE) a émis l'idée de la création d'un "euro numérique[423]". Justifié par l'ampleur de ces actifs dans l'économie contemporaine et inspiré par d'autres initiatives à travers le monde[424], la BCE a mis en marche un processus d'investigation devant aboutir en 2023 ou 2024. Dans l'hypothèse de son adoption, cette monnaie permettrait aux citoyens et entreprises de la Zone euro de payer directement par le biais de cette devise, à l'instar de l'euro traditionnel.

255.- Bien que les détails précis de ses caractéristiques ne soient pas encore arrêtés, *"l'euro numérique sera, quoi qu'il en soit, émis par la Banque centrale européenne et circulera dans des porte-monnaies électroniques ou « wallets », indépendamment des autres moyens de paiement[425]"*. La question qui se pose est dès lors de savoir quelles seraient les conséquences en matière de criminalité de cette crypto-monnaies centralisée. A priori, les risques inhérents à la blockchain publique pourraient être atténués par le contrôle exercé par la BCE. Celle-ci aurait la maîtrise de la production de ces actifs et pourrait même en suivre l'utilisation, ce qui faciliterait le travail des enquêteurs dans le cadre d'investigations sur des infractions liées à des fraudes ou des blanchiments d'euros virtuels. L'efficacité de la répression s'en trouverait renforcée.

256.- Néanmoins, deux failles sont d'ores et déjà décelables. Tout d'abord, l'instauration d'une crypto-monnaie officielle ne supprimerait pas le recours aux crypto-monnaies décentralisées. Au contraire, ces dernières pourraient même connaître un intérêt renouvelé en ce qu'elles permettraient de contourner la surveillance institutionnelle. De plus, des questions se posent s'agissant des risques en matière de vie privée des utilisateurs. Dans sa présentation du projet, la CNIL soulignait - citant en cela les recommandations du GAFI quant à ce projet[426] - *"qu'en ce qui concerne les monnaies numériques de banque centrale, un équilibre est à trouver entre la LCB-FT et la protection de la vie privée et des données personnelles[427]"*. Face au dualisme fondateur entre sécurité et liberté, la balance se devra donc d'être équilibrée pour que les libertés individuelles ne soient pas sacrifiées

[423] "Report on a digital euro", BCE, octobre 2020.
[424] Notamment celle de la Suède avec son e-krona, des États-Unis avec le e-dollars ou de la Chine avec son e-yuan.
[425] "Euro numérique : quels enjeux pour la vie privée et la protection des données personnelles ?", CNIL, 14 février 2022.
[426] FATF (2020), FATF Report to the G20,
[427] "Euro numérique : quels enjeux pour la vie privée et la protection des données personnelles ?", préc.

sur l'autel de la recherche des infractions et la protection de l'ordre public. Cette exigence sera donc la clé de lecture de la recevabilité d'un tel projet dans une société démocratique.

Paragraphe 2. Le Parquet européen, acteur central de la lutte contre la criminalité 3.0

En s'affranchissant des frontières des États membres de l'UE, le Parquet de Luxembourg dispose d'une compétence territoriale générale sur tout le ressort européen[428]. En outre, il dispose d'un domaine de compétence matériel recouvrant les infractions que la blockchain et plus spécifiquement la crypto-monnaie, peuvent favoriser (A). Enfin, les prérogatives qu'il tient de la loi lui permettraient de donner à ces faits une réponse ferme et véloce (B).

A. Une compétence matérielle adéquate

257.- Au sein de l'écosystème des parquets spécialisés, la création d'un ministère public à compétence exclusive et transnationale pour connaître des infractions portant atteinte aux intérêts financiers de l'Union européenne[429] est l'innovation la plus récente à laquelle la France a apporté son adhésion[430]. Reposant sur une architecture à la fois autonome - le parquet européen est dirigé par un procureur européen indépendant des États membres - et décentralisée - le ministère public européen se divise pour chaque États en un procureur européen basé à Luxembourg et de procureurs européens délégués installés dans chaque pays membres - cette nouvelle autorité judiciaire sera dans la lutte contre la criminalité 3.0 une force vive. Plus précisément, la compétence de ce parquet concerne à titre exclusif[431]:

- Fraude financière au budget européen > 10000 euros
- Fraudes à la TVA >10 millions d'euros de préjudices en lien avec le territoire de 2 États membres ou plus.
- Soustraction, Détournement, destruction de biens publics
- Blanchiment de capitaux, contrebande, importation ou exportation frauduleuse
- Corruption d'agents publics nationaux et de l'UE.

[428] A tout le moins pour les pays ayant adhéré à cette institution.
[429] Règlement (UE) 2017/1939 du Conseil du 12 octobre 2017 mettant en œuvre une coopération renforcée concernant la création du Parquet européen
[430] LOI n° 2020-1672 du 24 décembre 2020 relative au Parquet européen, à la justice environnementale et à la justice pénale spécialisée
[431] F. CHOPIN, support de cours sur le parquet, Master 2 sécurité intérieure 2022-2023.

258.- Toutes ces infractions financières ont pour particularité d'être en lien avec la crypto-monnaie. Ainsi, qu'il s'agisse de blanchiment par crypto-actifs, de soustraction ou détournement de ce dernier, voire de corruption d'agent par leur intermédiaire, la compétence du parquet européen pourra être activée lorsque les intérêts financiers européens seront menacés, *id est*, lorsqu'un préjudice aura été subi de la part de l'Union européenne ou l'une de ces institution. En outre, l'adoption éventuelle d'un euro numérique soulèverait d'autres questions de compétence pour ce parquet. Il serait en effet possible de caractériser des fraudes au budget européen commises par détournement de subventions elles-mêmes versées sous cette devise. La crypto-monnaie ne serait plus l'instrument mais l'objet de l'infraction.

B. Des prérogatives renforcées au service de la poursuite des infractions commise par la blockchain

259. Quelle que soit la forme de l'atteinte, le rôle de cette autorité judiciaire serait cardinal. Le propre de la criminalité blockchain étant sa rapidité de commission et de dissimulation, toute perte de temps est superfétatoire et rend l'issue des poursuites toujours plus incertaine. Ainsi, malgré une efficacité caractérisée, la coopération européenne traditionnelle apparaît peut-être trop lente face à l'immédiateté qu'impose cette nouvelle technologie. Dès lors, la capacité d'action d'une autorité centrale sur tout le territoire des États membres - par le truchement de ses délégués - offre une perspective d'accélération de la lutte inestimable. De même et sur le plan interne, la complexité des schémas infractionnels permis par la blockchain nécessite généralement l'ouverture d'une information judiciaire. Cette étape supplémentaire est néanmoins inutile dans le cadre des infractions sus énoncées en ce que les procureurs délégués disposent - à quelques exceptions près[432] - des mêmes prérogatives qu'un juge d'instruction conformément aux articles 696-114 et suivants du Code de procédure pénale. Ce dernier *"s'habille des vêtements du juge d'instruction en l'autorisant à définir lui-même des placements sous contrôle judiciaire, à mettre en examen, à procéder à des interrogatoires et confrontations, des auditions de témoins en ce compris les témoins assistés, de décider de la recevabilité de la constitution d'une partie civile ou encore à délivrer des mandats de comparution ou d'amener[433]"*.

[432] Notamment en ce qui concerne les mesures de placement sous assignation à résidence sous surveillance électronique ou en détention provisoire pour lesquelles seul le juge des libertés et de la détention est compétent.
[433] C. POTIER, "Le procureur européen délégué, Janus judiciaire ?", *Actu juridique, Lextenso*, 14 février 2020.

260.- Malgré ces perspectives d'espoir dans l'efficacité de ce parquet, il n'est pour l'heure pas possible d'affirmer avec certitude qu'elles s'avèreront en pratique. En raison d'une adhésion incomplète des États de l'Union à cette institution - 23 sur 27 - de la limitation de son champ matériel de compétence à certaines infractions ainsi que du maintien d'un niveau étatique de poursuite - et partant de souveraineté pénale - ce parquet pourrait souffrir de lacunes face aux nouveaux défis de la blockchain. Partant, faudrait-il étendre son champ de compétence aux infractions commises en ligne ? Comment penser la coopération de cette entité avec les pays non adhérents ? Toutes ces interrogations seront tributaires de la pratique et devront être appréhendées de façon progressive.

Conclusion du Titre I

261.- Ainsi, il ressort de l'analyse non exhaustive[434] des dispositifs internationaux et européens de lutte contre la criminalité liée à la blockchain que la coopération est une variable indispensable. Elle permet de saisir des actes autrement inatteignables et de les poursuivre nonobstant les frontières. Toutefois, la rapidité avec laquelle ces infractions peuvent être commises et celle avec laquelle leurs auteurs peuvent disparaître impose également une réponse nationale dimensionnée à ces nouveaux enjeux. Il en va de la pérennité du système économique dans son ensemble tant l'essor des crypto-monnaies apparaît inéluctable (**Titre II**).

[434]N'ont notamment pas été évoqués certains mécanismes de coopération tels que le mandat d'arrêt européen, les demandes d'entraide pénale européenne ou encore les diverses demandes de reconnaissance d'acte en ce que ces mesures n'appellent pas de précision particulières quant à leur application à la criminalité 3.0. Elles sont en effet susceptibles d'être mises en œuvre de manière classique.

Titre II. Une réponse pénale nationale fondée sur l'adaptation

262.- Face à l'appropriation par les organisations criminelles des nouvelles technologies aux fins de commission d'infractions, une réponse équivalente doit être apportée par les autorités répressives. Pour lutter à armes égales, les États sont tenus de développer des techniques innovantes de nature à permettre l'administration de preuves volatiles, l'appréhension d'individus inexistants et la saisie de biens immatériels. Pour ce faire, c'est l'ensemble de la procédure pénale et du droit pénal de fond qu'il faut repenser. D'une part, l'enquête pénale au sens large - définie comme l'ensemble des investigations destinées à recueillir des éléments suffisamment probants pour établir la matérialité des faits et la culpabilité de leur auteur - devra nécessairement s'adapter à ce nouveau paradigme de criminalité. Elle devra mobiliser toute l'ingénierie humaine afin de pouvoir répondre au défi technologique qui se fait jour et devra pour cela moderniser le modèle classique d'investigation (**Chapitre 1**). D'autre part, et parce que la procédure pénale n'est qu'une arme au service du droit pénal de fond, celui-là devra être repensé afin de pouvoir appréhender ces nouvelles formes de criminalité. Or, l'un des buts du droit pénal est de punir[435]. Partant, la dématérialisation de la répression devra également être poursuivie (**Chapitre 2**).

Chapitre I. La modernisation des investigations

262.- Des Travaux et des Hommes[436]. La procédure pénale est - du moins pour l'instant - mise en mouvement et conduite par des humains. Elle repose donc fondamentalement sur leur capacité individuelles et collectives à enquêter et identifier les indices *"graves et concordants rendant vraisemblable qu'elles aient pu participer, comme auteur ou comme complice, à la commission des infractions[437]".* Aussi, c'est par leur expérience et leur expertise que ces derniers peuvent offrir une plus-value à la poursuite des infractions. C'est donc aussi par leur spécialisation qu'ils peuvent

[435] C. pén., art. 130-1 : " Afin d'assurer la protection de la société, de prévenir la commission de nouvelles infractions et de restaurer l'équilibre social, dans le respect des intérêts de la victime, la peine a pour fonctions :
1° De sanctionner l'auteur de l'infraction ;
2° De favoriser son amendement, son insertion ou sa réinsertion".
[436] Référence au poème d'Hésiode *Les Travaux et les Jours*.
[437] C. pro. pén., art. 80-1.

s'adapter à la criminalité nouvelle et y répondre efficacement (**Section 2**). Cependant, pour mener à bien leur œuvre inquisitrice, les acteurs de la procédure pénale se fondent sur des techniques d'enquête. Celles-ci prenant des formes variables en fonction de la nature des preuves à obtenir. Néanmoins, toutes sont tenues à une amélioration constante, corrélative à l'amélioration des criminels dans leur praxis. La progression technologique des techniques d'enquête est donc essentielle en matière de criminalité blockchain (**Section 1**).

Section 1. L'amélioration des techniques d'enquête

263.- L'amélioration des techniques résulte d'une double dynamique. Dans un premier temps, il importe de renouveler les moyens déjà existants et qui ont démontré leur efficacité depuis leur introduction dans le droit français. Afin de les rendre opératoires dans un contexte de numérisation de la criminalité, l'adaptation de ces techniques classiques est cardinale (**Paragraphe 1**). Mais pour saisir toutes les formes nouvelles d'infraction, notamment celles recourant aux crypto-monnaies ou au Métavers, il semble que de nouvelles techniques ad hoc doivent être employées en lien avec la technologie qui soutient cette infrastructure : la blockchain (**Paragraphe 2**).

Paragraphe 1. Une adaptation des techniques d'investigation existantes

264.- Il serait difficile et surtout inutile de recenser tous les dispositifs dont la mise en œuvre devrait être renouvelée au prisme de la blockchain. Aussi, le choix sera fait de mettre en lumière deux des techniques d'investigations les plus usitées et les plus efficaces. Dans ce contexte, seront d'abord envisagées les perquisitions et saisies. Ces deux actes qui sont en réalité quasiment indivisibles devront en effet être modulés afin de prendre en compte le caractère dématérialisé des transactions réalisées par la blockchain (A). En parallèle, la recherche d'informations sur les auteurs potentiels d'infractions commises par la blockchain pourrait être complexifiée au regard de la décentralisation inhérente à son usage. Il pourrait être en effet difficile de savoir à qui adresser une réquisition (B).

A. Les perquisitions et saisies au prisme de la dématérialisation des transactions

265.- Les perquisitions et saisies sont des actes de procédure par lesquels le domicile d'un individu est visité et les biens ou éléments présents éventuellement recueillis par les enquêteurs. Plus précisément, il s'agit pour ces derniers de "*rechercher dans un lieu normalement clos, tous les indices permettant d'établir l'existence d'une infraction ou d'en déterminer l'auteur*[438]". Quoi qu'il en soit, ces mesures soulignent l'aspect matériel des opérations et l'exigence de corporéité des indices. Cette première acception n'est pas incompatible avec la blockchain.

266.- Il existe plusieurs formes de conservations des crypto-monnaies[439]**.** En effet, bien qu'elles soient conservées sur ce qu'il est communément admis de qualifier de portefeuille, ces derniers se présentent sous des aspects divers. Ils peuvent notamment être matérialisés dans des outils physiques appelés également *cold wallet*[440] ou *hardware wallet*. Il s'agit d'un mode de conservation sûr en ce que le propriétaire des crypto-monnaies les place à l'abri d'un piratage. C'est également une faiblesse dès lors que ce support - qui peut prendre des formes variées telles qu'une clef USB ou un QR-code - peut faire l'objet d'un vol mais également d'une saisie pénale.

267.- Aussi, identifier ces outils de stockage est essentiel pour le déroulement de l'enquête et les enquêteurs doivent être capables de ne pas passer à côté. Pour ce faire, il leur faut prêter attention à tous éléments de nature à revêtir cette caractéristique de stockage et apprendre à identifier les nouvelles formes adoptées par les criminels, lesquels ne manqueront pas d'innover pour tromper leur vigilance.

268.- Une fois identifiés, il est donc possible de saisir ces portefeuilles. Mais pour quel usage ? C'est ici qu'intervient l'Agrasc[441] afin de procéder à la vente des biens saisis et, en l'espèce, des crypto-actifs. Pour ce faire, l'agence devra avoir au préalable créer un portefeuille sur lequel seront

[438] F. DEBOVE, F. FALLETTI, I. PONS, *Précis de droit pénal et de procédure pénale,* Major, 2022, p. 839.
[439] Pour être exact, il s'agit en réalité de la conservation des clefs permettant d'accéder aux crypto-monnaies.
[440] bitFlyer.com, Glossaire "Cold storage" : "Un cold wallet, aussi connu sous le nom de cold storage, fait référence à une méthode de stockage hors ligne de monnaies virtuelles".
[441] Agence de gestion et de recouvrement des avoirs saisis et confisqués créée par la loi du 9 juillet 2010 visant à faciliter la saisie et la confiscation en matière pénale.

transférés les actifs numériques[442]avant leur aliénation[443] dans le cadre d'une vente aux enchères publique. Toutefois, nonobstant l'obtention de ce portefeuille, il faut pouvoir accéder à son contenu. Or, ce dernier est protégé par un code d'accès indispensable. Serait-il possible de contraindre un individu à le révéler ?

269.- L'article 434-15-2 du Code pénal sanctionne *"le fait, pour quiconque ayant connaissance de la convention secrète de déchiffrement d'un moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit, de refuser de remettre ladite convention aux autorités judiciaires ou de la mettre en œuvre, sur les réquisitions de ces autorités ..."* Cette disposition, déclarée conforme au principe de la présomption d'innocence et plus particulièrement au droit de garder le silence et de ne pas s'incriminer soi-même[444], pourrait s'appliquer en l'espèce eu égard à l'acception libérale de la Chambre criminelle quant à la nature de la convention secrète. Dans un arrêt d'assemblée plénière du 7 novembre 2022, elle précise en effet que *"la convention de déchiffrement, visée par ce texte - l'article 434-15-2 du Code pénal-, s'entend de tout moyen logiciel ou de toute autre information permettant la mise au clair d'une donnée transformée par un moyen de cryptologie, que ce soit à l'occasion de son stockage ou de sa transmission[445]"*. Partant, le refus opposé par le détenteur de la clef privée - qui est ici assimilable à la convention de déchiffrement visée par le texte - pourrait être contraint d'en révéler la teneur, à peine de sanction lorsque les portefeuilles sont conservés sur un smartphone - ce qui est souvent le cas.

---

[442] "Questions à Olivier Le Guen sur la perquisition et la saisie des crypto-actifs" in Dossier : La justice pénale à l'épreuve des cryptomonnaies, *Dalloz IP/IT,* 2019.

[443] Conformément à l'article 41-5 du Code de procédure pénale qui prévoit que *"lorsqu'au cours de l'enquête la restitution des biens meubles saisis et dont la conservation n'est plus nécessaire à la manifestation de la vérité s'avère impossible, soit parce que le propriétaire ne peut être identifié, soit parce que le propriétaire ne réclame pas l'objet dans un délai de deux mois à compter d'une mise en demeure adressée à son dernier domicile connu, le juge des libertés et de la détention peut, sur requête du procureur de la République et sous réserve des droits des tiers, autoriser la destruction de ces biens ou leur remise au service des domaines aux fins d'aliénation".*

[444] Décision n° 2018-696 QPC du 30 mars 2018

[445] Cour de cassation, Assemblée plénière, 7 novembre 2022 pourvoi n° 21-83.146

B. L'identification des organismes aux fins de réquisitions, un défi inhérent au caractère décentralisé de la blockchain

270.- Les portefeuilles peuvent aussi être dématérialisés. Dans ce cas, ils sont conservés sur un logiciel adapté, lequel peut être géré directement par le propriétaire ou par un prestataire de services[446]. Cet intermédiaire dispose donc des crypto-monnaies d'un individu, lesquelles pourraient être saisies dans le cadre d'une procédure pénale. Néanmoins, pour accéder à son contenu, il faut d'abord obtenir la communication des données de connexion du client, ce qui amène d'abord à définir exactement la nature de cette demande et par extension son régime.

271.- L'article 77-1-1 - dans le cadre de l'enquête préliminaire qui sera prise comme référence - permet au procureur de la République ou à un officier de police judiciaire, sur autorisation de ce magistrat, de solliciter *"toute personne, de tout établissement ou organisme privé ou public ou de toute administration publique qui sont susceptibles de détenir des informations intéressant l'enquête (...) de lui remettre ces informations, notamment sous forme numérique"*. Il s'agit ici des traditionnelles réquisitions faites auprès d'entités dépositaires d'informations nécessaires à l'enquête - également possible en enquête de flagrance et en instruction. Or, la question pourrait se poser de savoir si les PSAN sont susceptibles de faire l'objet de telles réquisitions. Le texte vise parmi les données demandées "des informations" dès lors qu'elles sont ou paraissent utiles à l'enquête. Aussi, il est permis d'entendre dans cette notion les informations relatives au portefeuille d'un client.

272.- Solution partielle. À l'instar de la perquisition, l'obtention des données relatives à un portefeuille ne sera pas suffisante pour y accéder. Il demeurera subordonné à l'obtention de la clef privée qui seule permet de saisir et transférer les crypto-monnaies. De plus, et comme il a été précédemment souligné[447], une grande partie des transactions de crypto-actifs se font encore de manière décentralisée, c'est-à-dire, sans passer par un intermédiaire de type PSAN ou en passant

[446] Ainsi, nombreux sont les gestionnaires de portefeuilles de crypto-actifs - PSAN - qui offrent des services de conservation mais aussi d'investissement tels que Coinhouse, Etoro, Cryptobjectif ou encore Rivemont.
[447] Voir n°252.

par un PSAN[448] situé à l'étranger[449]. Il s'agit pour l'instant d'une des limites de ce système d'enregistrement qui n'a pas encore trouvé de solution[450].

Paragraphe 2. Des techniques nouvelles reposant sur la blockchain

273.- Au-delà d'une simple adaptation des moyens traditionnels d'enquête - qui pourraient dans l'absolu être tous aménagés aux fins de s'adapter à la blockchain - il paraît intéressant de se demander si des dispositifs ad hoc ne pourraient pas être employés. A l'évolution de la criminalité s'opposeraient une révolution des investigations fondée sur la technique. Deux idées forces seront mobilisées.

274.- D'une part, la plasticité de la blockchain suscite l'intérêt des acteurs - répressifs et scientifiques - dans le cadre d'une utilisation orientée vers la recherche probatoire. Seraient potentiellement permises des techniques reposant directement sur son fonctionnement (A).

275.- D'autre part, la fracture conceptuelle incarnée - ou désincarnée - par le Métavers fait sourdre l'idée d'un renouvellement des structures classiques de l'investigation pénale, laquelle devrait se mouvoir dans ce nouvel univers immatériel et transcendantal (B).

A. L'usage de la technologie blockchain, exemple de la neutralité technologique

276.- Le principe de neutralité technologique signifie qu'un moyen technologique n'est, a priori, affecté d'aucun coefficient de nocivité ou de bonté. Il est donc conditionné par l'utilisation qui en est faite et les applications dont il fait l'objet. La blockchain est, à cet égard, de même nature et peut par conséquent donner lieu à un usage salutaire. Elle pourrait notamment servir en tant que moyen de preuve.

277.- Deux sortes de preuves peuvent être distinguées[451]. Les preuves en source ouverte qui résultent de la participation de toutes personnes - publiques officielles, publiques médiatiques -

[448] Selon un rapport du 31 mai 2021 fourni par l'ACPR, parmi les 19 PSAN enregistrés en France, le volume de transaction traité s'élevait à 204 millions d'euros pour 198 millions d'actifs conservés. Or, selon ce rapport, le taux de pénétration des crypto-actifs est sans doute bien plus important. ACPR, Rapport annuel 2021.
[449] Dans ce cas, une demande d'entraide pénale internationale ou une décision d'enquête européenne est requise.
[450] Il faudrait pouvoir identifier toutes les transactions dont celles effectuées entre acteurs décentralisés. C'est pour l'heure impossible eu égard au nombre de transactions quotidiennes dont la majorité sont licites.
[451] G. VIAL, O. LECLERC, E. VERGES, Preuves scientifiques et technologiques, Cahiers, Droit, Sciences et Technologies, Presses universitaires d'Aix-Marseille, 2020, pp.209-226

volontaires ou involontaires. Plus simplement, les informations en source ouverte sont *"les données numériques disponibles par une simple recherche sur Internet, sur un réseau social, dans des bases de données publiques (et qui) peuvent nourrir l'enquête pénale et constituer des éléments de preuve dans le cadre d'un litige*[452]*",* et qui sont communément qualifiée d'OSINT - Open Source Intelligence (1). À côté de ces sources ouvertes, des sources plus traditionnelles dites fermées existent. Elles sont *"soit conservées sur des supports qui sont physiquement inaccessibles au public (dans un domicile, un bureau), soit elles sont contenues dans un système informatique connecté à un réseau, mais protégées par un code d'accès*[453]*"*. L'apport de la blockchain pourra là encore être interrogé (2).

1. L'OSINT et la blockchain

278.- Le développement des médias de grande ampleur et plus récemment des réseaux sociaux a créé ce que Bernard HARCOURT nomme la "société d'exposition[454]". Les informations circulent en effet librement et rapidement à travers Internet et peuvent parfois constituer des sources majeures dans le cadre d'enquêtes pénales. Par exemple, l'enquête menée par l'ONG *Bellingcat* et le site d'investigation en ligne *Correct!v* concernant le crash de l'avion MH17, a-t-elle permis de déterminer que l'avion avait été abattu par un missile russe[455]. De même, l'enquête diffusée dans l'émission Africa Eye de BBC Africa "Anatomy of a killing[456]" et montrant une vidéo d'exécution de femmes et d'enfants dans une région d'Afrique - dont le lieu et le moment exacts furent identifiés grâce à l'intervention de plusieurs internautes visionnant les images - fut une illustration des possibilités offertes par cette information ouverte.

279.- L'une des failles de ce système informationnel est relative à la fiabilité des données. Le Haut-commissariat des Nations unies aux droits de l'homme et l'université de Berkeley ont publié un protocole[457] afin d'orienter le travail des enquêteurs en open source[458]. Car, même si la preuve produite par des particuliers est affranchie de l'obligation de loyauté[459], celle-ci doit être

[452] Ibid.
[453] Ibid.
[454] B. E. HARCOURT, *La société d'exposition. Désir et désobéissance à l'ère numérique,* Paris, Seuil, 2020.
[455]R. ROUMANOS, « Les promesses et les défis journalistiques de l'*Open Source Intelligence* (OSINT) », *I2D - Information, données & documents*, 2021/1 (n° 1), p. 45-50.
[456] https://youtu.be/XbnLkc6r3yc (Les images peuvent heurter).
[457] G. THIERRY, « Comment la justice travaille avec les recherches en sources ouvertes », *Dalloz actualité*, 8 juill. 2022.
[458] *Berkeley Protocol on Digital Open Source Investigations: A Practical Guide on the Effective Use of Digital Open Source and Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law*
[459] Crim. 15 juin 1993, pourvoi n° 92-82.509.

suffisamment fiable pour emporter l'intime conviction du juge. À cet égard, le protocole recommande notamment aux enquêteurs de conserver les données - ce qu'il qualifie de "reproductibilité de l'enquête[460]" - afin d'être en mesure de produire ces éléments et de préciser leurs sources. Dans ce contexte, l'apport de la blockchain serait déterminant. En tant que registre public et inaltérable, elle permettrait de retracer la source des informations produites et inscrites par des tiers pour renforcer leur poids devant le juge pénal. La question serait alors celle de la recevabilité d'une preuve dans un tel support. Or, le principe posé à l'article 427 du Code de procédure pénale ainsi que la conception compréhensive de la Chambre criminelle concernant la liberté de la preuve offrent une assise stable en faveur de ce mode de preuve.

2. Blockchain et preuves fermées

280.- Si par principe la blockchain est publique et donc accessible erga omnes - ce qui permet ainsi la traçabilité des transactions en crypto-monnaies et l'identification finale de leur détenteur - certaines structures sont fondées sur un système fermé à protection renforcée. Ces blockchains dites privées soulèvent dès lors des défis en matière d'investigation.

281.- Peut-on perquisitionner la blockchain ? L'article 706-102-1 du Code de procédure prévoit *"qu'il peut être recouru à la mise en place d'un dispositif technique ayant pour objet, sans le consentement des intéressés, d'accéder, en tous lieux, à des données informatiques, de les enregistrer, de les conserver et de les transmettre, telles qu'elles sont stockées dans un système informatique, telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de traitement automatisé de données, telles qu'il les y introduit par saisie de caractères ou telles qu'elles sont reçues et émises par des périphériques".* Il s'agit de la pénétration par les enquêteurs - dans le cadre de la poursuite d'une infraction entrant dans le champ de la criminalité organisée - sur un système informatique afin de suivre en temps réel l'activité numérique de son utilisateur.

281.- La blockchain privée imperméable à toute intrusion ? Le processus de fonctionnement de la chaîne de blocs apparaît rétif à toute immixtion de l'extérieur. Pour intégrer la blockchain, il faudrait procéder à une étape préalable consistant en l'installation d'un logiciel espion - de type Cheval de Troie ou Pegasus - par l'envoi d'un message piégé - technique du hameçonnage - sur l'ordinateur de l'individu disposant des codes d'accès à cette structure. Mais il s'agirait là d'une

[460] O. LECLERC, *Jalons prospectifs sur l'exigence de reproductibilité dans la recherche juridique,* in Mélanges en l'honneur de Pascal ANCEL, Larcier, LexisNexis, 2021, p. 177

voie détournée passant par l'utilisation classique d'une technique existante. De même, il serait possible pour des enquêteurs habilités à cet effet d'intégrer la blockchain privée en recourant à un pseudonyme conformément à l'article 230-46 du Code de procédure pénale. Là encore, aucune intrusion directe dans la blockchain privée ne serait constatée car l'agent l'intégrerait par autorisation d'un tiers dont il aurait gagné la confiance. Par conséquent, il semble bien que les mesures d'enquête portant directement sur la blockchain privée soient impossibles.

B. La maîtrise du Métavers, enjeu fondamental de la lutte

282.- Il existe des infractions commises dans le Métavers[461]. Aussi, il devrait corrélativement exister des investigations dans cet espace virtuel. Or, comme l'ont montré les précédents développements, il semble nécessaire de prendre en compte divers aspects de cet univers pour y mener des enquêtes.

283.- L'anonymat qui règne dans le Métavers constitue en lui-même une difficulté probatoire. En effet, qu'il s'agisse de la Cour de cassation[462] ou de la Cour européenne des droits de l'homme[463], le principe du contradictoire - lequel découle du principe des droits de la défense - fait obstacle à ce que les preuves soumises à l'appréciation des juges proviennent de sources occultes. Malgré des dérogations limitées aux procédures en lien avec la criminalité organisée, ce principe devrait donc exclure la prise en compte des indices et preuves obtenus dans le Métavers. Aussi, il serait souhaitable d'imaginer un cadre d'enquête dérogatoire destiné à saisir cette particularité afin de concilier l'efficacité des investigations et le respect des droits de la défense.

284.- La transcendance du Métavers est une donnée à prendre en compte dans la perspective d'une adaptation de la répression pénale. Elle fait naître la question de l'accès à la preuve. En ce que les interactions qui s'y opèrent sont dépourvues de support matériel extérieur, elles pourraient ne pas être suffisamment tangibles pour être produites dans le cadre d'une enquête. La question de la loyauté de la preuve ressurgira également dès lors que les procédés d'obtention pourront demeurer opaques. Par conséquent, le recours à la blockchain pourrait être une solution eu égard à son rôle d'authentification des informations et d'horodatage des échanges. Par exemple, un procès-verbal pourrait être rédigé et enregistré dans cette structure, laquelle lui garantirait une

[461] Voir n° 49.
[462] Cass. Crim., QPC, 9 nov. 2010, inédit, pourvoi n° 10-82.918
[463] CEDH 20 nov. 1989, *Kostovski c. Pays-Bas*, requête n°11454/85.

existence certaine. Cette transcendance souligne aussi les exigences d'adaptation de la coopération internationale au regard de la décentralisation intrinsèque à cette technologie, accessible en tout point du globe.

285.- Un usage didactique du Métavers peut enfin être attendu et est déjà expérimenté. Ainsi, Interpol[464] a mis au point son propre Métavers destiné à la formation des enquêteurs en réalité augmentée. Ce projet - également poursuivi par Europol[465] - a pour objet de préparer les forces de l'ordre au développement des "métacrimes" susceptible de se multiplier à l'avenir. Des lieux sont matérialisés afin d'accueillir les agents et les soumettre à des mises en situation. Face au retard pris par les pouvoirs publics par rapport aux organisations criminelles les plus puissantes dans le domaine des nouvelles technologies, l'utilisation d'armes équivalentes sera un prérequis indispensable.

Section 2. La spécialisation des acteurs de la chaîne pénale

286.- Dans la conception grandissante de l'efficacité en matière répressive, la spécialisation est devenue une exigence première. Il s'agirait en cela d'un principe nouveau de procédure pénale fondé notamment sur les besoins d'adaptation à une criminalité innovante, usant des dernières possibilités offertes par la technique et répondant à des schémas d'action jusque-là inédits. Dans ce tropisme, les acteurs de la sécurité intérieure doivent s'adapter qu'ils soient publics (**Paragraphe 1**) ou privés (**Paragraphe 2**).

Paragraphe 1. L'adaptation des agents de sécurité publique

Schématiquement, il est possible de distinguer les services d'enquête (A) des autorités judiciaires (B). S'ils partagent tous deux le même objectif de préservation de l'ordre public, ils n'agissent pas dans le même registre ni avec les mêmes moyens. Dès lors, c'est par complémentarité que leurs activités respectives se manifestent.

[464] "INTERPOL launches first global police Metaverse", Interpol, 20 octobre 2022.
[465] "Policing in the metaverse: what law enforcement needs to know", Europol, 21 octobre 2022.

A. Une prise en compte par les services d'enquête des typicités de la blockchain

287.- Les enquêteurs stricto sensu s'entendent des agents étatiques affectés à titre principal ou exclusif à la poursuite des auteurs d'infraction. Sont ainsi exclus les agents des douanes - dont la mission peut certes recouvrir les enquêtes mais concerne surtout le contrôle des marchandises et des personnes - les personnels de l'administration pénitentiaire, ainsi que les fonctionnaires des administrations dotés de prérogatives en matière d'investigation mais dont la mission première est autre[466]. Seront donc ici visés les agents de police nationale (1) et de gendarmerie (2).

1. La police nationale face à la criminalité 3.0

288.- L'une des caractéristiques de la police nationale est son architecture fondée sur une répartition des compétences au sein de directions ou de sous-directions. Ainsi, elle est capable de couvrir tout le champ de la criminalité et d'affecter à un domaine en particulier des moyens matériels et humains adaptés. Dans le cadre des infractions commises par le prisme de la blockchain, c'est la Sous-direction de lutte contre la cybercriminalité - SDLC - qui est qualifiée. Créée en 2014, elle se compose de 150 agents affectés dans plusieurs divisions[467]. Au sein de la SDLC, l'Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication - OCLCTIC - fait figure de pivot de la lutte contre toutes les formes de cybercriminalité. Elle permet la mise en oeuvre de coopérations internationales par le biais de sa section coopération ; l'impulsion d'enquêtes grâce à sa section opérationnelle - notamment en matière de ransomware et de trafics commis sur le Darknet ; la détection des phénomènes criminels par le biais des signalements recueillis sur la plateforme PHAROS[468] et surtout THÉSÉE[469].

289.- Dans le domaine plus particulier des crypto-monnaies, la doctrine d'adaptation aux nouvelles technologies de la police nationale lui permet de conserver une effectivité dans les enquêtes et de ne pas passer à côté d'éléments a priori insignifiants. Pour ce faire, les formations des agents ont intégré depuis les années 2010 les notions de base de la blockchain - afin d'établir un

---

[466] Tel est le cas notamment des agents du Fisc, des caisses de sécurité sociale, de l'ONF ou encore de l'Inspection du travail.

[467] "Sous-direction de lutte contre la cybercriminalité", Police nationale.intérieur.gouv.fr.

[468] Plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements, un site web créé le mardi 16 juin 2009 par le Gouvernement français pour signaler des contenus et comportements en ligne illicites, (https://fr.wikipedia.org/wiki/PHAROS). Celle-ci trouvera peu à s'appliquer en ce qui concerne les infractions relatives à la blockchain, à l'exception des cas d'enregistrement de contenu illicite dans cette dernière.

[469] Le traitement harmonisé des enquêtes et signalements pour les e-escroqueries (THÉSÉE) est destiné à recueillir les plaintes des victimes d'escroquerie commises en ligne afin de les centraliser et de les répartir entre services compétents. Elle pourrait notamment trouver un usage dans le cadre des escroquerie à l'investissement en crypto-monnaies.

niveau commun de connaissance - ainsi que des dispositifs plus complexes - destinés à des fonctionnaires spécialisés[470]. Aussi, c'est forte de cette expertise que la police nationale a pu récemment appréhender un individu pour blanchiment de crypto-actifs en lien avec un rançongiciel et saisir près de 19 millions d'euros d'actifs numériques[471].

2. La technicité de la gendarmerie confrontée au défi de la blockchain

290.- La gendarmerie nationale s'est progressivement inscrite dans le mouvement général de perfectionnement des forces de sécurité intérieure face aux enjeux évolutifs de la criminalité. S'agissant des nouvelles technologies, sa figure de proue est le Centre de lutte contre la criminalité numérique - C3N - rattaché à la police judiciaire de la gendarmerie nationale[472]. Composé de 54 membres, il contribue à l'action cyber destinée à lutter contre les infractions commises par ces nouveaux vecteurs. Il s'est récemment fait connaître pour son action dans l'affaire dite Encrochat, au terme de laquelle *"les conversations non chiffrées et en temps réel d'environ 60 000 utilisateurs et près de 120 millions de messages et images, presque tous liés à de la criminalité organisée de haut niveau, ont été interceptés, sans que la captation soit détectée[473]"*. Le dispositif d'interception très sophistiqué mis en place par le C3N démontre son expertise.

291. La problématique des crypto-monnaies a été assimilée avec force par cette entité qui a acquis des compétences reconnues en la matière[474]. Capable de retracer les transactions effectuées sur la blockchain et de démanteler les réseaux de blanchiment. Elle a notamment contribué au succès d'investigations menées en coopération avec les autorités américaines, Europol ainsi que les autorités néerlandaises et belges, afin de saisir la plateforme d'échange Bitzlato le 19 janvier 2023. Ce sont 700 millions de dollars d'échanges illicites qui ont justifié cette opération de grande envergure. Ce succès souligne l'apport de la gendarmerie à la coopération internationale et la reconnaissance de son haut degré de compétence.

---

[470] "Formation des forces de Police à la blockchain : entretien avec le Major Erwan Bouliou", Crypotast.fr, 30 septembre 2022, consulté le 20 janvier 2022.
[471] "La police a saisi 19 millions d'euros sous forme de crypto actifs issus de ransomwares, l'Usine digitale.fr, 16 décembre 2021, consulté le 20 janvier 2022.
[472] S. BERNARD, "La montée en puissance de l'investigation cyber en gendarmerie", gendarmerie.interieur.gouv.fr, 28 janvier 2020, consulté le 20 janvier 2022.
[473] "Retour sur l'affaire EncroChat, ou quand les cyber-gendarmes ont hacké la messagerie chiffrée utilisée par la criminalité organisée", Bureau des affaires criminelles de la gendarmerie nationale, 29 juillet 2020, consulté le 20 février 2023.
[474] La gendarmerie nationale a même eu recours à la crypto-monnaie Tezos pour valider et certifier des transactions financières.

B. Les nouveaux défis des autorités judiciaires

292.- La spécialisation des autorités judiciaires répond à celle de la criminalité et des criminels[475]. A cet égard, le professeur Serge GUINCHARD soulevait dans une contribution de 2010[476] que : "l'accroissement *de la technicité de certains contentieux, plus exactement leur complexité, engendre un besoin de spécialisation des juges".* C'est donc par nécessité que les compétences des juges et plus généralement celles des juridictions sont de plus en plus poussées dans un champ précis. La blockchain et ses dérivés interrogent ainsi sur la nécessité de créer un nouveau bloc de compétences ad hoc ou au contraire de l'intégrer au sein d'une catégorie plus vaste.

293.- Il existe déjà une spécialisation des juridictions et des procédures en matière de cybercriminalité. En effet l'article 706-72 du Code de procédure pénal précise que *"Les infractions mentionnées aux articles 323-1 à 323-4-1 et 411-9 du code pénal, lorsqu'elles sont commises sur un système de traitement automatisé d'informations, sont poursuivies, instruites et jugées selon les règles du présent code sous réserve du présent titre".* Sont ici visées les atteintes aux STAD dont il a été démontré qu'elles pouvaient englober les atteintes contre la blockchain. De plus, depuis la loi du 23 mars 2023[477], la Juridiction National de Lutte contre la Criminalité Organisée - JUNALCO - est spécialement chargée des affaires de cybercriminalité d'une très grande complexité[478]. Parmi ces dernières, il est notamment important d'intégrer les schémas de blanchiment par crypto-monnaies qui, par leur caractère occulte et international, imposent la poursuite par une juridiction à compétence nationale. Il en va de même pour les atteintes aux STAD précitées. Cette spécialisation sera également cardinale pour que les différents acteurs intervenant dans le domaine de la criminalité 3.0 - dont l'ANSSI fait partie - d'avoir un interlocuteur identifié avec lequel échanger des informations[479].

---

[475] N.CATELAN, "La spécialisation des juridictions pénales", in Colloque : " Faut-il déspécialiser la procédure pénale ?" Faculté de droit de Nancy, mars 2016.
[476] S.GUINCHARD, "Rapport de synthèse" in *La spécialisation des juges,* Presses de l'Université Toulouse 1 Capitole, LGDJ - Lextenso Éditions, 2012.
[477] LOI n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice.
[478]Circulaire du 17 décembre 2019 relative à la compétence nationale concurrente du tribunal de grande instance et de la cour d'assises de Paris dans la lutte contre la criminalité organisée de très grande complexité, et à l'articulation du rôle des différents acteurs judiciaires en matière de lutte contre la criminalité organisée.
[479]Groupe de travail présidé par B. SPITZ , "LE DROIT PÉNAL À L'ÉPREUVE DES CYBERATTAQUES", avril 2021.

294.- Mais cette spécialisation est-elle suffisante ? Permet-elle de saisir toutes les problématiques que soulève la blockchain et ses émanations ? Dans l'hypothèse d'une réponse négative et de la nécessité subséquente de créer un nouveau bloc de compétences propre à cette technologie, il est possible d'imaginer que la juridiction - ou plutôt la section - chargée de poursuivre et de réprimer les faits soit composée de magistrats spécialement formés en la matière, avec notamment un parquet dédié et des juges d'instruction préposés. Il serait aussi exigé une spécialisation de la phase de jugement avec une composition pourvue en conséquence. Mais cet idéal de se heurte aussitôt à la réalité matérielle. Le déficit de magistrats en général ne permettra pas d'affecter certains d'entre eux à ces enjeux si particuliers et dont le poids total dans la criminalité n'est pas encore substantiel. Il serait préconisé la poursuite d'une formation généralisée à tous les magistrats afin qu'ils aient une compréhension a minima de la blockchain. La poursuite et le jugement des infractions y afférentes devraient rester dans le giron des sections déjà existantes du tribunal judiciaire de Paris lorsqu'elles sont d'une certaine complexité.

Paragraphe 2. L'apport technique des acteurs privés de sécurité

Si l'intervention du secteur privé dans le domaine de la lutte contre la criminalité blockchain peut s'entendre au regard de l'origine libertarienne de cette technologie (A), l'abandon de ce champ d'action à ces acteurs n'est ni souhaitable ni même possible (B).

A. Une expertise avérée des acteurs privés de la sécurité

295.- Née dans le secteur privé, la blockchain est avant tout une institution de relation pair-à-pair créée pour des particuliers. Il est donc cohérent qu'elle soit maîtrisée au premier chef par ces derniers. Ainsi, nombreuses sont les sociétés à avoir investi dans ce domaine et à y avoir développé leur expertise. Dans cette logique commerciale de la blockchain, dont les crypto-monnaies sont l'exemple le plus abouti, la question de la sécurité s'est également imposée. Les acteurs privés, qui connaissent un essor depuis les années 1960 aux États-Unis et 1990 en France, sont aujourd'hui des agents parallèles de la sécurité. En France par exemple, ce sont quasiment 185000 agents qui sont dénombrés, avec une forte croissance devant conduire à un effectif équivalent à celui des acteurs publics[480].

[480] "La sécurité privée en France", Defense-Zone. com, 11 mai 2022, consulté le 20 janvier 2022.

296.- La maîtrise de la blockchain couplée aux exigences sécuritaires qu'elle fait naître a incité certaines entreprises à se spécialiser dans la détection et la révélation des phénomènes criminels 3.0. L'exemple de Chainalysis est sans doute le plus parlant. Fondée en 2014, cette société se propose d'analyser les infractions commises par et contre la blockchain et de réaliser des synthèses à destination des gouvernements et des agents des forces de l'ordre. Son rapport annuel sur la criminalité en matière de crypto-monnaies, le "Crypto crime report[481]", offre une présentation quantitative et qualitative très détaillée de ces phénomènes. En outre, elle réalise des investigations au profit des autorités étatiques et a permis de remonter la trace de nombreux auteurs par l'usage des crypto-monnaies.

B. Une privatisation nécessairement circonscrite de la sécurité

297.- Cette utilisation de Chainalysis et des autres prestataires de service met en lumière la coopération salutaire entre la sécurité publique et privée. Elle s'inscrit dans le cadre du continuum de sécurité prôné depuis la loi du 25 mai 2021[482] qui fait de la complémentarité un paramètre essentiel de l'efficacité répressive. Toutefois, cette intervention soulève en contrepoint des critiques en termes d'accessibilité - eu égard à son coût qui constituerait un frein pour les particuliers suspectés à la différence des autorités publiques - source de rupture d'égalité des armes ; de la collecte massive de données qu'elle est capable de mettre en place sans contrôle réellement effectif ou encore sur l'origine de ses sources qui sont peu transparentes. Son aide, bien que précieuse, doit donc être circonscrite aux faits les plus complexes appelant par là même la plus grande technicité.

298.- La sécurité est avant tout une mission de l'État entendu comme incarnation de la puissance publique. En effet, aux termes de l'article L. 111-1 du Code de la sécurité intérieure : *"la sécurité est un droit fondamental et l'une des conditions de l'exercice des libertés individuelles et collectives. L'État a le devoir d'assurer la sécurité en veillant, sur l'ensemble du territoire de la République, à la défense des institutions et des intérêts nationaux, au respect des lois, au maintien de la paix et de l'ordre publics, à la protection des personnes et des biens"*. Dans ce contexte, le Conseil constitutionnel se montre attentif à ce que ce dernier ne délègue pas de prérogatives pour lesquelles il dispose d'un monopole. Ainsi, la volonté de permettre à des agents privés de visionner

[481] Voir à cet égard le dernier rapport "Crypto-crime 2022" à cette adresse : https://go.chainalysis.com/2022-Crypto-Crime-Report.html.
[482] LOI n° 2021-646 du 25 mai 2021 pour une sécurité globale préservant les libertés.

les images de vidéosurveillance de la voie publique avait-elle était censurée par le Conseil Constitutionnel, dans sa décision du 10 mars 2011, en ce que, "*permettre de déléguer à des personnes privées l'exploitation et le visionnage de la vidéoprotection, aboutirait à confier à des personnes privées la surveillance générale de la voie publique et ainsi à leur déléguer des compétences de police administrative générale inhérentes à l'exercice de la « force publique*[483]*"*. C'est donc la notion plus générique de force publique qui constitue, semble-t-il, le critère de partage entre acteurs publics et privés de la sécurité.

300.- Quid de la blockchain ? Eu égard à sa plasticité, cette technologie est susceptible de recouvrir des aspects divers, dont certains sont liés à des prérogatives de puissance publique. Il n'est qu'à penser aux domaines économique et financier. Est-il possible de laisser au secteur privé la liberté absolue de mettre en place un marché parallèle de devises telles que les crypto-monnaies ? Dans le cadre de la sécurité, l'utilisation de la blockchain dans la collecte et la gestion de données sensibles - telles que celles relatives à la santé ou au secret des affaires - par des acteurs privés peut également être contestée. Aussi, il faut poser comme principe d'action la coopération du secteur privé avec le public et non la domination de l'un sur l'autre. C'est par un juste équilibre que l'objectif commun de sécurité pourra être atteint.

Conclusion du Chapitre 1

300.- Adaptation des techniques et spécialisation des acteurs sont donc deux voies dans l'amélioration globale de la lutte contre la criminalité par la blockchain. Elles se répondent nécessairement tant le développement d'outils plus performants doit s'accompagner d'une augmentation de la qualification des agents destinés à les utiliser, au premier rang desquels les services d'enquête. Mais au-delà de cet aspect formel, c'est également le versant plus substantiel du droit pénal de fond qui doit être repensé (**Chapitre II**).

[483] n° 2011-625 DC du 10 mars 2011

Chapitre II. La dématérialisation de la répression

299.- Après avoir analysé le droit pénal spécial de la blockchain dans la première partie, puis souligné quelques particularités de procédure pénale propres à celle-ci, il convient de clore ce travail de recherche par une réflexion portant sur le droit pénal général, entendu comme *"l'ensemble des règles juridiques qui organisent la réaction de l'État vis-à-vis des infractions et des délinquants*[484]*"*. Sont donc visés les principes généraux relatifs à l'infraction, la culpabilité, l'imputabilité et la peine.

300.- Blockchain et responsabilité pénale. Reposant sur des conditions d'engagement précises, la responsabilité pénale se distingue de la responsabilité civile par une conception stricte. Fondée sur des principes généraux - dont nombre d'entre eux sont de valeur constitutionnelle - elle est intrinsèquement liée à la réalité matérielle. Un auteur est ou n'est pas pénalement responsable s'il est établi - ou non - qu'il a commis une infraction punissable et qu'il est en mesure de répondre de ses actes. Partant, l'apparition de la blockchain comme nouveau paradigme de criminalité met en tension ces principes acquis qui doivent faire l'objet d'une reconceptualisation nécessaire (**Section 1**).

301.- Pénologie de la blockchain. Cette discipline qui concerne *"l'étude des mesures pénales et des effets qui en résultent, tout particulièrement en ce qui concerne la protection de la société et la réintégration sociale des délinquants*[485]*",* recèle également un intérêt conceptuel dans son application à la criminalité blockchain. En ce que cette technologie sous-tend des éléments dont la matérialité est parfois évanescente, la mise en œuvre concrète des peines traditionnelles peut s'avérer plus complexe. Dès lors, ce sont les modalités des sanctions pénales qui devront être repensées à l'aune de cette criminalité (**Section 2)**.

[484] R. MERLE, A. VITU, *Traité de droit criminel,* Cujas 7e édition, 2000, n°146.
[485] G. THINES et A. LEMPEREUR, *Dictionnaire général des sciences humaine*s, Paris, Éditions universitaires, 1975

Section 1. Une responsabilité pénale à reconceptualiser

302.- Parce que l'engagement de la responsabilité pénale d'un individu n'est que la résultante d'un rituel immuable et garant de la sécurité juridique, plusieurs phases sont au préalable exigées avant de pouvoir conclure à sa certitude. Le droit pénal repose sur des considérations de souveraineté en ce qu'il est *"l'expression de l'autorité du souverain à l'égard de sa population et de son territoire*[486]*"*. Il est donc fondamentalement un droit de l'État et son application démontre la capacité de ce dernier à réguler les facteurs de trouble à son ordre public. Parce qu'il est un droit de souveraineté, le domaine de compétence territoriale de la loi pénale française doit être déterminé avec précision. Or, s'agissant de la blockchain, il peut être difficile, voire impossible, d'identifier l'un des critères de rattachement classiques qui régissent les rapports entre États (**Paragraphe 1**).

303.- Nonobstant l'identification de la juridiction compétente, il est ensuite nécessaire de pouvoir établir le lien qui relie l'homme au fait criminel. Car le principe est celui de la personnalité de la responsabilité pénale[487], il faut, au terme du processus judiciaire, pouvoir avec suffisamment de conviction, identifier le ou les auteurs de l'infraction. Cette imputation déjà source de difficulté en temps normal, prend des allures de gageure lorsqu'elle doit composer avec des concepts aussi lâches que ceux offerts par la blockchain. La difficile appréhension des personnes responsables ne doit toutefois pas en décourager l'exploration (**Paragraphe 2**).

Paragraphe 1. Réflexion sur l'application de la loi pénale française

304.- L'application dans l'espace de la loi pénale repose sur des critères précis. Présentés dans la partie générale du Code pénal, ils sont fonction de la nature des infractions, de la valeur des intérêts en jeu ou encore de la qualité des victimes ou des auteurs. Toutefois, au sein de cette multitude de critères de rattachement, le principe de territorialité émerge avec force (A). À ses côtés, d'autres fondements sont marginalement prévus afin de suppléer à une territorialité affaiblie ou concurrencée (B).

[486] *LA SOUVERAINETÉ PÉNALE DE L'ETAT AU XXIÈME SIÈCLE,* Colloque annuel de la Société française pour le droit international, Lille , 18, 19 et 20 mai 2017.
[487] C. pén., art. 121-1 : *"Nul n'est responsable pénalement que de son propre fait"*.

A. Conciliation du principe de territorialité et de la blockchain

305.- Aux termes de l'article 113-2 du Code pénal, *"la loi pénale française est applicable aux infractions commises sur le territoire de la République. L'infraction est réputée commise sur le territoire de la République dès lors qu'un de ses faits constitutifs a eu lieu sur ce territoire"*. Deux phrases, deux principes : celui de la compétence de la loi française à l'égard des infractions commises sur le territoire de la République ; celui de l'assimilation du fait constitutif au tout. En conséquence, la compétence française à l'égard de la criminalité blockchain dépendra de cette double exigence de détermination de son lieux de commission (1) et de l'identification de ce lieu comme constitutif du territoire de la République (2).

1. La détermination du lieu de commission de l'infraction face à l'a-territorialité de la criminalité

306.- Les infractions liées à la blockchain sont par nature décentralisées. *"La technologie de la blockchain, à laquelle recourent les actifs numériques, repose sur le principe d'un registre décentralisé, ce qui a pour conséquence que les informations relatives à une unité de valeur sont partagées parmi les ordinateurs qui constituent le réseau, sans que celles-ci puissent être assignées à l'un d'entre eux ou certains d'entre eux de façon permanente*[488]*"*. Par extension, une opération réalisée sur la blockchain ne pourra pas être reliée à un pays en particulier dès lors qu'elle met en relation toute la communauté mondiale. Un échange de bitcoins à des fins de blanchiment par exemple, peut permettre d'identifier les adresses de l'émetteur et du récepteur. Or, outre la possibilité pour eux de recourir à des systèmes de mixeurs pour effacer l'origine de la transaction, il n'est pas possible de déterminer avec précision le lieu de réalisation de l'infraction car elle résulte d'une validation par des milliers d'ordinateurs répartis sur la planète[489].

307.- Mais cette aporie première n'est pas inéluctable. Tout d'abord, il serait possible d'identifier l'intermédiaire d'une telle transaction lorsqu'il prend la figure d'un prestataire de services sur actifs numériques. Les PSAN sont en effet des entités prenant généralement la forme de sociétés et donc disposant d'un siège social, d'une immatriculation et d'une réalité matérielle. L'attribution de la compétence territoriale pourrait donc être fondée sur la territorialité de ce prestataire[490]. L'autre

[488] J. GOLDSZLAGIER – A. LE TEURNIER, "La lutte contre le blanchiment à l'épreuve de la territorialité des crypto-actifs", AJ Pénal, 2021, 465

[489] Même si les plus grandes fermes à minage sont situées dans quelques pays identifiés comme la Chine, les États-Unis ou la Russie.

[490] Avec cependant la limite déjà évoquée du recours encore résiduel des utilisateurs de crypto-monnaies à ces prestataires.

possibilité[491] serait de fonder la compétence territoriale sur le lieu de conservation de la clef privée, qui bien que distincte de la transaction litigieuse, n'en est pas moins le moyen d'accès. Ces clefs pouvant être stockées sur un support matériel ou logiciel, cette identification pourra être plus ou moins délicate.

2. L'identification du territoire de la République dans l'espace numérique

308.- Le législateur définit le territoire français *comme devant inclure également "les espaces maritime et aérien qui lui sont liés[492]".* Cette conception extensive omet cependant un espace infractionnel nouveau et pourtant capital : l'espace numérique. Comment en effet faire correspondre la commission d'une infraction dans le cyberespace avec la notion de territorialité ? Cela revient à s'interroger sur l'existence d'un cyberespace indépendant de l'espace géopolitique matériel - ce qui dépasserait le cadre de ce mémoire - mais également de déterminer les critères de rattachement entre le monde virtuel et le monde réel.

309.- La solution est relativement simple lorsque l'infraction commise a mobilisé un réseau de communication électronique. Dans ce contexte, l'article 113-2-1 dispose que le crime ou le délit *"lorsqu'il est tenté ou commis au préjudice d'une personne physique résidant sur le territoire de la République ou d'une personne morale dont le siège se situe sur le territoire de la République, est réputé commis sur le territoire de la République".* Il s'agit donc d'une compétence territoriale aménagée pour prendre en considération les intérêts de la victime et se rapprochant ainsi d'une compétence personnelle passive. Dans le cas de la criminalité 3.0, ce critère pourra trouver à s'appliquer à chaque fois qu'une victime est identifiée, notamment dans le cadre des atteintes aux biens commises en ligne tels que les vols ou les ransomware.

309.- Le Métavers, espace indépendant ou territorialement identifiable ? Cet univers est quant à lui source de plus de difficultés. En ce qu'il se veut transcendant et permanent, le Métavers est décorrélé d'une quelconque territorialité. Il constitue son propre territoire et obéit à ses propres lois. De plus, l'accès à cet espace virtuel peut se réaliser depuis tout endroit de la planète. Partant, il serait inenvisageable en l'état de pouvoir déterminer le lieu exact auquel il est lié. Ce sont d'autres critères de compétence qu'il faudrait invoquer pour pouvoir saisir la criminalité qu'il permet.

[491] Op. cit, J. GOLDSZLAGIER et A. LE TEURNIER.
[492] C.pén., art. 113-1.

B. Pertinence des critères alternatifs dans l'appréhension de la criminalité 3.0

310.- Outre le critère de la territorialité de la compétence, d'autres critères attributifs sont prévus afin de cibler des situations dans lesquelles la gravité et la complexité des faits imposent de récuser le lieu de commission. Au regard de la particularité des infractions reposant sur la blockchain, il est possible d'apprécier si et dans quelle mesure la compétence pénale de la loi française peut résulter de l'identité des protagonistes (1) ou de la nature des faits (2).

1. La compétence personnelle comme critère de compétence subsidiaire

311.- Deux formes de compétences personnelles sont classiquement distinguées par le Code pénal : la compétence personnelle active[493] liée à la nationalité de l'auteur et la compétence personnelle passive liée à la nationalité de la victime [494]- voire dans certains cas sont lieu de résidence[495]. Or, il semble permis de s'interroger sur l'efficacité de ces deux acceptions de la compétence ratione loci pour appréhender le phénomène criminologique de la blockchain.

312. - La compétence personnelle active permet de donner compétence à la loi française lorsque l'auteur de nationalité française à commis un crime ou un délit punit d'une peine d'emprisonnement hors du territoire de la République. A priori donc, ce système permettrait de saisir les faits commis à partir des fermes à mineurs situées à l'étranger et, partant, d'attraire les auteurs d'atteinte à la blockchain ou d'escroquerie dans le giron du juge répressif national.

Toutefois, deux tempéraments doivent immédiatement être relevés. Tout d'abord, il est nécessaire pour les délits que les faits constituent également une infraction dans le pays de commission[496]. Or, dans un domaine où les conceptions relatives à la blockchain sont marquées du sceau de l'hétérogénéité, il paraît douteux qu'une réciprocité puisse être atteinte. De plus, et pour les délits également, les poursuites ne peuvent avoir lieu qu'à l'initiative du ministère public et après *"plainte de la victime ou de ses ayants droit ou d'une dénonciation officielle par l'autorité du pays où le fait a été commis[497]"*. Là encore, cette restriction à la compétence française qui fait de l'initiative de la victime ou des autorités locales une condition sine qua non de la répression, semble peu soluble dans l'exigence d'immédiateté que ces infractions supposent. Il s'agit d'une solution plus théorique

[493] C. pén., art. 113-6.
[494] C. pén., art. 113-7.
[495] C. pén., art. 113-2-1 en matière d'infraction commise par le biais d'un réseau de communication informatique.
[496] C.pén., art. 113-6 al. 2.
[497] C. pén., art. 113-8.

que pratique dont l'utilité serait circonscrite aux crimes - rares dans ce domaines - exonérés de ces conditions.

312.- La compétence personnelle passive est le pendant pour les victimes françaises de la compétence personnelle active. Si elle ne pose pas de condition de réciprocité de l'incrimination, elle exige toutefois l'action de la victime ou des autorités du pays. Elle se trouvera donc confrontées aux mêmes lacunes répressives, sous réserve des cas dérogatoires pour lesquels cette condition n'est pas requise[498].

313.- Problématiques communes. Pour mettre en œuvre l'un de ces deux critères, il faut préalablement résoudre une difficulté liée à l'anonymat offert par la blockchain. En effet, comment connaître la nationalité de l'auteur ou de la victime de l'infraction alors que son identité n'est pas établie. L'impunité des criminels et l'ignorance des victimes d'avoir subi une atteinte peuvent rendre cette détermination impossible. Ainsi donc, c'est dans une dimension très restreinte que ces deux alternatives pourraient trouver à s'appliquer, obligeant à imaginer une troisième voie.

2. Proposition d'un critère de compétence adapté à la blockchain

314.- Eu égard aux limites que connaissent les formes classiques d'attribution de la compétence française pour saisir cette criminalité, il est souhaitable de s'interroger sur l'instauration d'un critère ad hoc ou à tout le moins adapté. Plusieurs solutions pourraient être envisagées allant de la compétence réelle de la France en raison d'atteinte à ses intérêts fondamentaux en cas de falsification de monnaies[499] - bien que l'assimilation des crypto-monnaies aux monnaies légales soient discutables - la compétence en matière d'acte de terrorisme à l'encontre des auteurs de nationalité française ou résidant habituellement sur le territoire de la République[500] - notamment pour le financement du terrorisme par la crypto-monnaie ou encore le délit d'initié à caractère terroriste - ou encore la compétence de la loi française pour les infractions énumérées par

[498] Notamment lorsque l'infraction est commise, même depuis l'étranger, contre une victime française ou résidant habituellement sur le territoire de la République. Ces infractions limitatives doivent prévoir expressément la compétence de la loi française. Tel est le cas des infractions sexuelles sur mineur - article 222-22 al. 3 du Code pénal. Les infractions en matière de pédopornographie sur internet mobilisant la blockchain pourraient aussi être visées dès lors que l'article 113-2-1 vise indifféremment: "*tout crime ou tout délit réalisé au moyen d'un réseau de communication électronique"*.
[499] C. pén., art. 113-10.
[500] C. pén., art. 113-13.

l'article 113-14[501] du Code pénal lorsqu'elles portent atteinte aux intérêts financiers de l'Union européenne - ce qui pourrait être le cas si l'euro virtuel était adopté.

315.- Vers un nouveau cas de compétence universelle ? En ce que la technologie de la chaîne de blocs met à mal les conceptions traditionnelles de la territorialité en érigeant un espace décentralisé et dépourvu de tout lien de rattachement stable avec un quelconque État souverain, elle entre dans la catégorie de ces infractions qu'il appartient à tout pays de réprimer. Nonobstant une gravité bien moindre que les crimes visés par l'article 669-11 du Code de procédure pénale - crime de génocide, crimes contre l'humanité, crimes et délits de guerre - la criminalité 3.0 appelle de par sa décentralisation une réponse équivalente. Aussi, dans le cadre d'une convention internationale, les États signataires pourraient se voir imposer l'obligation de poursuivre ou d'extrader l'individu qui, se trouvant sur leur territoire, s'est rendu coupable d'une infraction par le truchement de la blockchain. Il s'agirait d'une application du principe de droit pénal international *aut dedere aut judicare.*

Paragraphe 2. La difficile appréhension des personnes responsables

316.- Après que la juridiction compétente a été déterminée, il faut identifier l'individu à l'encontre duquel il existe des charges suffisantes pour lui imputer la responsabilité de l'infraction. Il s'agit d'une étape essentielle à la déclaration de culpabilité et au prononcé éventuel d'une sanction pénale car, à l'inverse du droit civil, le droit pénal repose sur le principe de responsabilité personnelle[502]. Dans le champ infractionnel couvert par la blockchain toutefois, deux difficultés peuvent apparaître. Tout d'abord, les incertitudes relatives à la caractérisation des infractions déjà évoquées pour certaines d'entre-elles soulignent la question plus générale de l'application du droit pénal à des faits qui sont souvent méconnus. En effet, l'anonymat et l'opacité qui nimbent la blockchain font de cette dernière une zone d'ombre juridique dont il peut s'avérer problématique de se dégager. Plus concrètement, la question préalable qui pourrait se poser est celle de savoir si oui ou non une infraction à été commise (A). Mais nonobstant la conviction de l'existence d'une telle infraction, il pourra également être difficile d'identifier la personne qui, parmi les potentiels auteurs,

[501] Sont notamment visés l'escroquerie ; l'abus de confiance ; la soustraction, détournement ou destruction de biens ; la corruption d'agent public étranger ; le blanchiment de ces infractions. Toutes peuvent de manière plus ou moins directe viser la blockchain ou l'un de ses éléments.
[502] C. pén., art. 1211-1 préc.

devra in fine répondre de ses actes dès lors que le fonctionnement de la chaîne de blocs se fonde sur la décentralisation (B).

A. Une responsabilité pénale confrontée à l'incertitude

317.- Comment poursuivre ce qui ne se voit pas ? Cette question a priori théorique soulève en réalité des conséquences pratiques majeures en matière répressive. En effet, si la déclaration de culpabilité est l'aboutissement de l'action publique enclenchée par le ministère public[503] ou de l'action civile mise en mouvement par la victime[504], encore faut-il qu'un fait pouvant revêtir une coloration pénale puisse être identifié et donner lieu à des investigations. Or, par essence, les infractions réalisées par la blockchain sont silencieuses. Elles ne se dévoilent qu'en creux, par le constat d'un manque plus que par la détermination d'un préjudice. En particulier, les atteintes aux intérêts économiques - qui constituent la plus grande partie des infractions commises - sont la plupart du temps décorrélées de cette technologie. Les individus savent qu'ils ont subi un préjudice, mais ils ignorent d'où il provient.

318.- Détection des infractions en lien avec la chaîne de blocs. L'une des principales raisons de cette inertie résulte de ce que la blockchain est un système autonome et rapide. Les transactions s'y réalisent à grande vitesse - quelques secondes pour les plus rapides - et de manière relativement opaque. Or, pour déceler une infraction, il faut pouvoir identifier un fait ou un ensemble de faits isolés. Dans le système de flux actuel, cette opération peut s'avérer impossible. Seul le préjudice pourra être constaté sans que le fait générateur ne ressorte clairement. Ainsi, en cas d'atteinte, la victime pourra certes faire état des dommages par elle subis, mais sera incapable de les relier à une utilisation malveillante de la blockchain et a fortiori de l'attribuer à un individu précis. Dans le Métavers, cette rupture causale sera exacerbée par la virtualité des échanges réalisés. Les utilisateurs se trouveront confrontés à l'impossible établissement de l'origine de leur préjudice et ne pourront donc pas en demander la condamnation ni la réparation.

[503] C. pr. pén., art. 1er al.1.
[504] C. pr. pén., art. 1er al. 2.

319.- La présomption de causalité : solution à l'indétermination de la criminalité blockchain. Bien que le droit pénal soit par nature averse aux présomptions[505] sauf exceptions limitées[506], se sont développées des situations particulières dans lesquelles, bien que l'existence et l'origine de l'infraction soient quasiment certaines, il n'est pas possible de rattacher matériellement un résultat à son fait générateur. Ainsi, en matière de délinquance économique et financière, la loi du 6 décembre 2013[507] dite loi Sapin I, a créé dans le Code pénal une telle présomption. L'article 324-1-1 dispose en effet que *"pour l'application de l'article 324-1 - le blanchiment -, les biens ou les revenus sont présumés être le produit direct ou indirect d'un crime ou d'un délit dès lors que les conditions matérielles, juridiques ou financières de l'opération de placement, de dissimulation ou de conversion ne peuvent avoir d'autre justification que de dissimuler l'origine ou le bénéficiaire effectif de ces biens ou revenus".* Cette fiction juridique permet un renversement de la charge de la preuve - simple[508] - lorsque le flou et l'opacité qui entourent une opération financière font présumer son caractère infractionnel. Or, en matière de transaction par blockchain, dont il a été démontré qu'elles permettaient de blanchir des fonds de manière efficace, une telle présomption pourrait être aisément appliquée et même étendue à d'autres infractions économiques[509].

B. La responsabilité individuelle au miroir de la décentralisation

320.- De la lecture combinée des articles 121-1 et 121-4 du Code pénal, il se déduit que la responsabilité pénale est personnelle et individuelle. Personnelle en ce qu'elle vise avant tout une personne - qu'elle soit physique ou morale - et exclut a contrario la responsabilité des machines ou des animaux. Individuelle car elle vise le ou les auteurs d'une infraction et eux seuls. Or, la confrontation de ces deux principes avec la blockchain est source de frictions. Elle se heurte d'une part au caractère décentralisé de cette technologie qui efface l'existence de l'individualité de l'auteur et, d'autre part, à certains procédés découlant de la blockchain qui affectent la personnalité de ce dernier.

---

[505] Décision n° 99-411 DC du 16 juin 1999, cons 5 *"en principe le législateur ne saurait instituer de présomption de culpabilité en matière répressive"*

[506] Ibid, "*toutefois, à titre exceptionnel, de telles présomptions peuvent être établies, notamment en matière contraventionnelle, dès lors qu'elles ne revêtent pas de caractère irréfragable, qu'est assuré le respect des droits de la défense et que les faits induisent raisonnablement la vraisemblance de l'imputabilité"*

[507] LOI n° 2013-1117 du 6 décembre 2013 relative à la lutte contre la fraude fiscale et la grande délinquance économique et financière

[508] Pour répondre aux exigences tant du Conseil constitutionnel dans sa décision de 1999 que de la Cour européenne des droits de l'homme dans son arrêt Salabiaku contre France de 1988.

[509] Ainsi, il serait possible de présumer une corruption ou un favoritisme lorsque le paiement opaque d'un agent public est fait par crypto-monnaies. De même, une présomption de financement du terrorisme pourrait-elle s'appliquer lorsque de telles devises sont envoyées à un individu ou un groupement réputé terroriste.

321.- Le fonctionnement décentralisé de la blockchain signifie que plusieurs individus contribuent à son développement. Partant, *"chacun en a sa part et tous l'ont tout entier*[510]*"*. Aussi, il semble a priori difficile d'identifier la personne qui a matériellement commis une infraction par son truchement. De plus, des prestataires de services peuvent intervenir et renforcer cette incertitude. Dès lors, et à l'instar du régime prévu par la loi de 1881[511] sur la liberté de la presse, il pourrait être intéressant de créer pour les utilisateurs de la blockchain une "responsabilité en cascade[512] lorsque celle-ci permet notamment de diffuser des idées à caractère infractionnel - thèses antisémites, racistes, terroristes, vidéos ou images pédopornographiques etc. Ici, seraient au premier chef responsable : le gestionnaire du ou des portefeuilles incriminés, à défaut, l'intermédiaire ayant réalisé la transaction, à défaut, le ou les bénéficiaires de la transaction. Dans le Métavers, la solution serait analogue mais viserait en premier lieu l'hébergeur de l'univers virtuel - exemple de Facebook avec Méta - à défaut, le gestionnaire d'un environnement particulier au sein de cet univers incriminé - exemple d'une institution ou d'une entreprise agissant dans ce métavers - et in fine les utilisateurs - avec une incertitude sur la responsabilité de leur avatar.

322.- L'automatisation de certaines actions par le recours aux smarts contracts pourrait également être une faille dans l'identification de l'individu responsable. En programmant par avance dans la blockchain ces protocoles auto exécutoires, il serait possible de leur faire accomplir des actes contraires à l'ordre public[513] et partant répréhensibles, par des intelligences non humaines. Cette automatisation des tâches cumulée à l'anonymat des programmeurs est de nature à empêcher une identification précise de ces derniers. Aussi est-il nécessaire de revoir les modalités traditionnelles d'imputation de la responsabilité pénale en envisageant le cas échéant une forme détournée passant par le prisme d'une fiction juridique proche de celle prévue pour les

[510] V. HUGO, *Les Feuilles d'automne* (1831),
[511] Loi du 29 juillet 1881 sur la liberté de la presse

[512] Loi préc., art. 42 : *"Seront passibles comme auteurs principaux des peines qui constituent la répression des crimes et délits commis par la voie de la presse dans l'ordre ci-après, savoir :*

1° Les directeurs de publications ou éditeurs quelles que soient leurs professions ou leurs dénominations et, dans les cas prévus au deuxième alinéa de l'article 6, les codirecteurs de la publication ;

2° A leur défaut, les auteurs;

3° A défaut des auteurs, les imprimeurs ;

4° A défaut des imprimeurs, les vendeurs, les distributeurs et afficheurs".

[513] Par exemple la diffusion de fausses informations, l'envoi de messages malveillants, la saturation de systèmes informatiques etc.

présomptions de causalité. Ainsi, seraient responsables pénalement tous ceux qui ont contribué à la création ou la gestion de ces instruments, voire n'en sont que les exécutants. L'élément moral de l'infraction serait ici absorbé par sa matérialité, laquelle serait elle-même soumise à des distorsions insatisfaisantes en matière répressive.

323.- Ces conceptions certes théoriques et peut-être complexes tendent surtout à souligner comment le droit pénal général - ou spécial comme en matière de presse - doit s'adapter sans se renier pour embrasser ces nouvelles formes de criminalité. Cette évolution de la responsabilité doit in fine se répercuter sur l'adaptation des sanctions pénales.

Section 2. Des sanctions à adapter

324.- Sans prétendre à l'exhaustivité, il paraît important de réfléchir à une redéfinition des sanctions applicables pour les adapter aux particularismes de la chaîne de blocs. A l'issue d'une audience pénale deux demandes peuvent être formulées une fois la culpabilité retenue. Le ministère public requiert le prononcé d'une peine (**Paragraphe 1**) et la partie civile lorsqu'elle est présente sollicite le versement de dommages et intérêts (**Paragraphe 2)**. Ces deux temps du procès pénal doivent être interrogés à la lumière de la blockchain.

Paragraphe 1. La recherche d'une peine adéquate

325.- Le caractère principalement économique des infractions commises par le biais des instruments offerts par la blockchain permet de restreindre en conséquence la nature des peines qui seront les plus propices pour les réprimer. A cet égard, la peine de confiscation fait figure de peine de référence dès lors qu'elle peut s'appliquer aux crypto-actifs, nouvelles sources d'enrichissement pour les criminels (A). En outre, certaines sanctions non-pénales pourraient trouver à s'appliquer lorsqu'elles émanent d'autorités administratives chargées de la régulation des activités liées à la blockchain (B).

A. La saisie des crypto-monnaies comme peine de référence

326.- Afin que que l'adage *nemo ex delicto consequatur emolumentum*[514] soit consacré dans les faits, le droit pénal s'est transformé afin d'ériger en peine l'appréhension du patrimoine délinquant[515]. A ce titre, la peine de confiscation a été introduite au sein de l'article 131-21 du Code pénal afin de répondre aux objectifs fixés par le législateur et notamment l'idée selon laquelle "*la réussite d'une procédure pénale ne doit pas se mesurer seulement au nombre de personnes interpellées ou à la gravité des peines prononcées, mais aussi à la manière d'appréhender le patrimoine des délinquants*[516]*"*. Placée sous l'égide de l'Agence de gestion et de recouvrement des avoirs saisis et confisqués - Agrasc - la procédure de saisie et confiscation doit s'accommoder avec la nature particulière des crypto-monnaies.

327.- Que confisquer ? S'il est traditionnel de parler de la saisie avant la confiscation en ce qu'elle en est l'étape préalable, sera ici développée la réflexion portant sur l'objet sur laquelle elle portera en matière de crypto-monnaie et plus précisément, du titre auquel elle pourra être pratiquée. En effet, l'article 131-21 énumère les éléments de patrimoine pouvant être confisqués. Peuvent tout d'abord être concernés "*tous les biens meubles ou immeubles, quelle qu'en soit la nature, divis ou indivis, ayant servi à commettre l'infraction ou qui étaient destinés à la commettre*[517]*"*. Appliqué aux crypto-monnaies, il pourrait notamment s'agir des actifs porteurs de données à caractère pornographique, ceux destinés au financement du terrorisme ou encore au paiement des mandataires criminels. Plus généralement, seraient confiscables les crypto-monnaies lorsqu'elles servent de vecteur de l'infraction. Le texte vise également "*tous les biens qui sont l'objet ou le produit direct ou indirect de l'infraction*[518]*"*. Seraient ici visées les crypto-monnaies obtenues de manières frauduleuses ou violentes dans le cadre de vols, extorsions, escroqueries ou tout autre appropriation criminelle. De même il pourrait s'agir de saisir le produit d'un blanchiment réalisé par le biais de ces actifs, nonobstant la nature de l'infraction sous-jacente. Mais comment appréhender les mécanismes permettant de dissimuler ou de modifier la nature des crypto-monnaies tels que les mixages ou mélanges ? Face à cette interrogation, l'article susvisé n'apporte pas de solution satisfaisante en ce qu'il précise que *"si le produit de l'infraction a été mêlé à des fonds d'origine*

[514] Nul n'est censé tirer profit de son crime.
[515] LOI n° 2010-768 du 9 juillet 2010 visant à faciliter la saisie et la confiscation en matière pénale (1)
[516] J.-L. WARSMANN, AN, CR n°18, Prop. loi visant à faciliter la saisie et la confiscation en matière pénale, AN n° 1255, p. 2.
[517] C. pén., art. 131-21 al. 2.
[518] C. pén., art. 131-21 al 3.

licite pour l'acquisition d'un ou plusieurs biens, la confiscation peut ne porter sur ces biens qu'à concurrence de la valeur estimée de ce produit[519]. Ainsi, le juge devra estimer de manière quasiment prophétique quelle est la part des actifs qui est licite et celle qui découle d'une infraction. Enfin, et plus généralement, les crypto-monnaies pourront être confisquées lorsque le texte d'incrimination prévoit une confiscation de tout le patrimoine du criminel en tant que composante de celui-ci.

328.- Comment confisquer ? La confiscation n'est que l'étape finale de la procédure et constitue la peine stricto sensu. Tant que le prévenu ou l'accusé n'aura pas été définitivement condamné, il sera fait usage de la notion de saisie. Celle-ci, alors provisoire, sera confirmée sous la condition suspensive de la condamnation à la peine complémentaire de confiscation. Les saisies au cours de l'enquête ou de l'instruction ont lieu durant une perquisition comme cela a été vu précédemment[520]. S'agissant des crypto-monnaies, et hypothèse faite de leur identification par les services d'enquête, leur appréhension matérielle revêt une dimension problématique : la célérité. En effet, au regard de la volatilité fulgurante de ces actifs, qui peuvent s'apprécier ou se déprécier en l'espace de quelques heures, voire quelques minutes, il est fondamental de pouvoir les saisir rapidement pour pouvoir les vendre et ainsi pérenniser la valeur de la confiscation. Or, les modalités classiques de saisie au cours de l'enquête - autorisation du juge des libertés et de la détention sur requête du procureur de la République[521] - ou durant l'instruction - ordonnance de commission rogatoire du juge d'instruction - constituent des sources de lenteur incompatibles avec cette exigence. Aussi, l'une des propositions de la loi de programmation du ministère de l'Intérieure serait de permettre *"par dérogation à l'article 706-153, à l'officier de police judiciaire d'être autorisé, par tout moyen, par le procureur de la République ou par le juge d'instruction à procéder, aux frais avancés du Trésor, à la saisie d'une somme d'argent versée sur un compte ouvert auprès d'un établissement habilité par la loi à tenir des comptes de dépôts ou d'actifs numériques mentionnés à l'article L. 54- 10-1 du Code monétaire et financier"*. Ce n'est qu'à posteriori que *"le juge des libertés et de la détention, saisi par le procureur de la République, ou le juge d'instruction se prononce par ordonnance motivée sur le maintien ou la mainlevée de la saisie dans un délai de dix jours à compter de sa réalisation*[522]*"*. Cette accélération de la phase de saisie permettrait d'agir immédiatement dans le cadre de la

[519] C. pén., art. 131-21 al 3 in fine.
[520] Voir n°265.
[521] C. pro. pén., art. 706-153 : *"au cours de l'enquête de flagrance ou de l'enquête préliminaire, le juge des libertés et de la détention, saisi par requête du procureur de la République, peut autoriser par ordonnance motivée la saisie, aux frais avancés du Trésor, des biens ou droits incorporels dont la confiscation est prévue par l'article 131-21 du code pénal. Le juge d'instruction peut, au cours de l'information, ordonner cette saisie dans les mêmes conditions"*
[522] C. pr. pén., art. 706-154 dans sa version issue de la loi du 24 janvier 2023 d'orientation et de programmation du ministère de l'intérieur

découverte de ces actifs au cours d'une perquisition sans avoir à attendre l'autorisation de l'autorité judiciaire.

329.- La réalisation de la confiscation. L'Agrasc détient le monopole de la gestion et de la cession au profit du Trésor, des avoirs saisis et confisqués au cours de la procédure pénale[523]. Pour ce faire, elle organise des ventes judiciaires aux enchères publiques, donnant lieu à une forte médiatisation. S'agissant des crypto-monnaies, le montant des ventes réalisées atteignait 60 millions d'euros au 31 décembre 2022[524]. Ce montant important souligne la place que prennent progressivement ces biens meubles incorporels dans la criminalité et la nécessité consécutive pour les autorités publiques de les appréhender en utilisant les armes du droit. Cette peine de confiscation permet ici, par sa malléabilité et la diversité de ses applications, de correspondre à l'instrument coercitif par excellence.

B. Le pouvoir de sanction des autorité administratives

330.- Si la peine de confiscation tend à réprimer directement les auteurs d'infractions en lien avec la blockchain, les sanctions administratives que peuvent infliger certaines autorités administratives indépendantes - AAI - peuvent plus indirectement garantir la bonne mise en œuvre des mesures de vigilance destinées à prévenir la survenance de ces faits. Ces autorités peuvent se voir conférer des prérogatives importantes dans les domaines dont elles assurent la régulation. Leur pouvoir de contrainte se manifeste généralement sous la forme de sanctions administratives économiques dont les montants peuvent être très élevés. Comme il a été dit en amont de ces développements, les prestataires sur actifs numériques sont pour la plupart soumis à des obligations dans le champ des normes LCB-FT. Ils doivent également pour la plupart s'enregistrer et obtenir un agrément auprès de l'Autorité des marchés financiers et de l'Autorité prudentielle et de la concurrence. Ces deux entités disposent pareillement du pouvoir de sanctionner les manquements à ces obligations[525]. Ainsi, aux termes de l'article L. 561-36-1 du Code des marchés financiers, l'ACPR - de même que l'AMF - peut, en cas de constat d'une méconnaissance par les assujettis de leurs devoirs, prononcer une sanction pécuniaire *"dont le montant peut être fixé dans la limite du plus élevé des deux plafonds suivants : cent millions d'euros et dix pour cent du chiffre d'affaires*

[523]C. pr. pén., art. 706-160.
[524] J. BOURGAIS et C. OLIVIER, "La saisie pénale des actifs numériques: une saisie virtuelle ?" Gaz. Pal, 14 février 2023, n° 5.
[525]C. mon. fin., art. L. 561-36 1° et 2°.

total". Il s'agit ici d'une mesure très dissuasive de par son montant et qui assure par conséquent une incitation au respect des normes établies.

331.- Outre ces sanctions économiques directes, ces autorités peuvent également prononcer des sanctions disciplinaires telles que précisées à l'article L. 612-38 du CMF qui peuvent se cumuler avec les premières. Parmi celles-ci, la mesure la plus sévère est le retrait total d'agrément ou la radiation de la liste des personnes agréées qui constituent une espèce de privation des droits de la personne concernée. Appliquée aux PSAN qui ont l'obligation d'être agréés pour certains, il s'agit là d'une peine capitale. D'ailleurs, cette gravité justifie qu'un recours puisse être exercé à leur encontre. Il est en effet possible de saisir selon les cas la Cour d'appel de Paris - lorsque la sanction est prononcée par l'AMF[526] - ou le Conseil d'État - lorsqu'elle est prise par l'ACPR[527] - afin de contester de telles sanctions. L'intervention d'une autorité juridictionnelle offre ainsi la possibilité de bénéficier d'un contradictoire plus respectueux des droits de la défense que la simple décision administrative. De plus, *"lorsque les conséquences de la décision du régulateur apparaissent manifestement excessives ou remettent en cause la survie économique de l'acteur, ce dernier dispose de la possibilité d'avoir recours à des procédures d'urgence – le sursis à statuer devant la Cour d'appel de Paris et le référé suspension devant le Conseil d'État[528]".* Ainsi, dans trois ordonnances du 14 avril 2021[529], la Cour d'appel de Paris a prononcé le sursis à exécution des sanctions adoptées par l'AMF et consistant en la cessation par le PSAN de son activité en France.

Paragraphe 2. L'enjeux de la réparation des victimes

332.- Dans le processus pénal, la victime n'est pas négligée, loin s'en faut. En ce sens**,** elle dispose de la faculté d'être partie au procès pénal afin, d'une part, de soutenir l'accusation portée par le ministère public[530] et, d'autre part, de solliciter la réparation de son préjudice[531]. Pour autant, cette reconnaissance juridique de la victime ne se double pas systématiquement d'une prise en charge concrète. Parmi les raisons qui expliquent cette incurie, l'action des victimes peut être retardée, voire compromise, par la criminalité anonymisée que la blockchain rend possible (A). De

[526]C. mon. fin., art. L. 621-30.
[527]C. mon. fin., art. L. 612-16.
[528]"PSAN : Comment contester une décision du régulateur ?", ORWL Avocats, 4 mai 2021.
[529] CA Paris, pôle 5 - ch. 15, 14 avr. 2021, n° 20/18863.
[530] C. pr.pén., art. 1er. al 2 : *"cette action (publique) peut aussi être mise en mouvement par la partie lésée, dans les conditions déterminées par le présent code".*
[531] C. pr. pén., art. 2 : *"l'action civile en réparation du dommage causé par un crime, un délit ou une contravention appartient à tous ceux qui ont personnellement souffert du dommage directement causé par l'infraction".*

plus, et nonobstant la reconnaissance des victimes et leur participation au procès, les moyens de réparer des préjudices parfois inédits peuvent faire défaut, ou à tout le moins les laisser insatisfaites (B).

A. L'enjeux primordial de l'intervention des victimes

333.- Il est fréquent de recourir à l'expression "chiffre noir" pour désigner le nombre des personnes victimes d'une forme de criminalité dont le nombre estimé dépasse le nombre identifié. S'il est souvent fait état du chiffre noir massif concernant les violences à caractère sexuel[532], il pourrait également être très important s'agissant des infractions commises contre ou par la technologie blockchain. Si les estimations pour le premier semestre 2022 font état de 2 milliards[533] de dollars volés en crypto-monnaies, il est certain que la totalité des montants frauduleusement obtenus surpasse de beaucoup ce chiffre[534]. En effet, tant l'opacité des infractions (1) que l'inertie des pouvoirs publics (2) constituent des freins à l'action civile des victimes.

1. Percer l'obscurité pour faire valoir ses droits

334.- Les infractions commises par le biais des chaînes de blocs ou à leur encontre sont caractérisées par une opacité constitutive. Celle-ci résulte de la conjonction d'un pseudonymat de principe, d'une décentralisation fondamentale et parfois, de l'adjonction de dispositifs d'anonymat renforcés tels que le Darknet. Aussi, il est permis de considérer que la plupart des infractions en lien avec la blockchain sont de nature occulte. Or, le temps nécessaire à leur découverte représente pour les victimes - et les autorités de poursuite par analogie - un éloignement croissant de leur chance d'obtenir réparation ou répression. La prescription sexennale prévue pour les délits[535] - infractions les plus répandues dans ce domaine, nonobstant certaines hypothèses de qualifications criminelles - semble alors peu compatible avec cette situation. Pour prendre en compte cet inexorable écoulement du temps, la qualification de ces infractions occultes ou dissimulées permettrait de retarder le point de départ de l'action publique - et donc de l'action civile lorsqu'elle est portée devant le juridiction

[532] Selon le ministère de l'Intérieure, seuls 10 % des faits de violences sexuelles commises hors du cadre familial ont été portées à la connaissance des services sécurité en 2021 disponible sur le site officiel https://www.interieur.gouv.fr/actualites/communiques/violences-sexuelles-hors-cadre-familial-enregistrees-par-services-de.
[533] C. RUTH, "Crypto hackers stole almost $2 billion in H1 2022", Atlas VPN. com, 5 juillet 2022.
[534] L'organisme ne prend en compte que les vols et néglige donc les autres formes d'appropriation frauduleuses dont les escroqueries et les extorsions qui sont également très nombreuses.
[535] C. pr. pén., art. 8.

pénale[536]- *"à compter du jour où l'infraction est apparue et a pu être constatée dans des conditions permettant la mise en mouvement ou l'exercice de l'action publique[537]"*.

2. Être entendu par la justice

335.- Par le poids relativement faible qu'elles représentent au regard de l'ampleur des sommes concernées par cette criminalité, les victimes individuelles peuvent être confrontées à une certaine négligence de la part des autorités répressives. Parmi les affaires médiatisées relatives à la condamnation d'auteurs de vols ou de fraudes portant sur des crypto-monnaies ou des NFT, aucune ne concerne de petits épargnants ou investisseurs. Il s'agit généralement de montant colossaux - une tentative de blanchiment portant sur près de 3,6 milliards de dollars par un couple new-yorkais par exemple[538] - ou de grandes sociétés privées ou établissements publics, comme les hôpitaux ou les collectivités territoriales. Dès lors, comment éviter les classements sans suite en opportunité pour ces "petites victimes"?

336.- La voie associative pourrait ici être mobilisée. Le législateur ayant multiplié les cas dans lesquels une association régulièrement déclarée depuis une certaine durée - en général cinq ans - parfois agréée et se proposant par ses statuts d'agir en défense d'intérêts collectifs précis peut agir au nom d'une ou plusieurs personnes victimes. Il pourrait donc être décidé soit de créer un nouveau domaine d'intervention, soit d'inclure au sein d'une catégorie existante les actions à l'encontre des infractions commises au moyen de la blockchain, notamment au sein de celles relatives aux infractions terroristes s'agissant du financement du terrorisme par la crypto-monnaie ou encore à la corruption commise par ce vecteur.

B. Réparer les préjudices liés aux crypto-monnaies malgré leur volatilité

337.- L'un des points soulignés tout au cours de ces développements concerne la valeur fluctuante des actifs numériques. Reposant principalement sur la confiance, ils connaissent des variations d'une rapidité incommensurable. Or, parmi les mécanismes d'indemnisation des victimes d'infractions, et particulièrement en cas de soustraction, il est possible que leur soit restitué leurs

[536] C. pr. pén. art. 10.
[537] C. pr.pén., art. 9-1.
[538] "Les Etats-Unis ont saisi 3,6 milliards de dollars de bitcoins volés", Le Monde, 8 février 2022, consulté le 2 février 2023.

biens ou la valeur de ces derniers. Aussi, s'il s'agit de crypto-monnaies, durant le temps écoulé depuis la perte du bien et sa restitution à la victime, leur dépréciation à pu être très importante. Il est donc nécessaire de s'assurer de leur réalisation le plus rapidement possible afin que la valeur du produit de la vente soit pérennisée pour l'indemnisation. C'est là le rôle de l'Agrasc déjà évoqué qui peut être saisie par la victime dont le principe de la réparation a été admis par une décision définitive mais qui n'a pas encore été payée afin *"que ces sommes lui soient payées par prélèvement sur les fonds ou sur la valeur liquidative des biens de son débiteur dont la confiscation a été décidée par une décision définitive et dont l'agence est dépositaire*[539]*"*.

338. En sus de cette réparation traditionnelle, il est également envisageable de réfléchir à des modalités faisant directement intervenir la technologie blockchain. En effet, il serait notamment possible de générer un ICO à valeur préétablie et réactualisée le cas échéant dans le but unique d'indemniser les préjudices subis. Par exemple, la plateforme Harmony, spécialisée dans les crypto-monnaies, a proposé de mettre en circulation des "ONE" afin de réparer le préjudice subi par les victimes du hack de 100 millions de dollars de Horizon Bridge - son protocole - en juin 2022. Ici, la plateforme agirait comme un organisme d'indemnisation privée se substituant aux auteurs de l'infraction ainsi qu'aux mécanismes classiques tels que la CIVI. Il s'agirait de décentraliser la réparation en ce que le paiement des victimes serait tributaire de l'achat des jetons par les autres utilisateurs. Ainsi, l'idéologie sous-jacente - l'exclusion de l'État - de cette technologie retrouverait sa sublimation en permettant in fine de rétablir les victimes dans leur intégrité matérielle sans intervention de la puissance publique au stade de l'indemnisation.

339.- Sensibiliser les auteurs d'infractions par le Métavers. Afin de lutter contre les violences intrafamiliales et sexuelles, le ministère de la Justice a souhaité expérimenter auprès d'une trentaine de détenus une immersion en réalité virtuelle représentant l'évolution d'une situation conjugale en sept étapes, jusqu'au passage à l'acte[540]. Il s'agit ici de créer une forme d'électrochoc pour des individus déjà condamnés pour des faits similaires. Ainsi, c'est par l'évitement de la récidive que la réparation des victimes sera faite.

[539] C. pr. pén., art. 706-164.
[540] L. CARRIVE, "Quand la réalité virtuelle se met au service de la lutte contre les violences conjugales", Radio France, 24 janvier 2021.

340.- Blockchain et sanction ne sont donc pas antinomiques. Il est en effet possible, au prix d'une adaptation des principes fondamentaux de la répression, de saisir ce phénomène criminologique inédit. L'arsenal répressif existant ne semble pas appeler de bouleversement fondamental mais seulement une extension de son champ d'application. Si toutes les sanctions sont a priori susceptibles d'être prononcées, certaines semblent plus idoines. Tel est le cas de la peine de confiscation dont il a été vu qu'elle pouvait être utilisée pour saisir la source première de richesse de ces criminels : les crypto-monnaies. Le rôle de l'Agrasc sera ici central et elle devra réussir à appréhender de manière toujours plus fine ces nouveaux actifs.

341.- Au regard de la finalité particulière de l'action civile, il semble que la blockchain ne constitue pas un obstacle insurmontable mais bien au contraire un levier au service des victimes. Elle ouvre la voie à des formes plus rapides de paiement - par la célérité des transactions et leur possible automatisation - tout en garantissant leur intégrité - par une inscription dans un bloc immuable. Partant, elle répond à cette aspiration contemporaine de faire que la victime ne soit plus *"la grande oubliée du procès pénal*[541]*"*.

CONCLUSION DE LA DEUXIÈME PARTIE

343.- Comme il a su le faire face à d'autres formes évolutives de criminalité le droit pénal peut et doit répondre à la criminalité 3.0. Les procédures pénales dérogatoires et les techniques d'enquête sont d'ores et déjà présentes pour lutter contre cette forme spécifique de criminalité organisée et les sanctions existantes peuvent trouver à s'appliquer. La question la plus sensible reste celle de la responsabilité pénale dont il a été relevé que les conditions actuelles d'imputation étaient insuffisantes. Pour y remédier, des propositions concrètes ont été formulées, sans pour autant épuiser la réflexion. Enfin, le concept de sécurité global a été convoqué pour mettre en lumière les apports potentiels des acteurs privés dans ce domaine de haute technicité. Il en va de la systématicité de la réponse pénale et, partant, de la garantie d'une intégration sans risque de la technologie blockchain.

[541]R. CARIO, "De la victime oubliée ... à la victime sacralisée ?", *AJ Pénal 2009* p.491

CONCLUSION GÉNÉRALE

344.- Au gré de ces développements, plusieurs idées forces ont pu être identifiées. Tout d'abord, la blockchain et les dispositifs qu'elle alimente sont des technologies neutres, voire positives. Ses usages bénéfiques dépassent en effet largement les détournements à des fins criminelles. Aussi, bien que ce travail de recherche tende à analyser les contours de la criminalité qu'elle fait craindre, il ne remet pas en cause cette innovation. Seuls les aspects néfastes de cette dernière ont été exacerbés afin d'en souligner la menace, ce qui ne doit pas faire croire à un outil intrinsèquement illicite.

344.- La criminalité évolue plus rapidement que le droit. Il est désormais acquis que les nouvelles technologies sont plus facilement appréhendées et maîtrisées par les auteurs d'infractions que par les pouvoirs publics. Cette spécialisation des criminels propre aux sociétés organiques dont parlait Émile DURKHEIM[542] leur assure un temps d'avance sur les services répressifs chargés de gérer l'ensemble du spectre infractionnel. Toutefois, cet état de fait ne doit pas conduire au fatalisme. Si certaines infractions sont rendues possibles par la blockchain et constituent ainsi une rupture conceptuelle, la plupart ne sont que des formes accélérées et anonymisées d'infractions existantes. Aussi, les modes de raisonnement et les qualifications doivent évoluer pour saisir les premières mais peuvent directement s'appliquer aux secondes.

345.- La France est l'un des pays les plus investis dans le domaine de la régulation des crypto-actifs. Elle dispose d'un cadre législatif et réglementaire substantiel - largement inspiré des recommandations du GAFI et de l'Union européenne - mais également d'un cadre répressif propre reposant sur la spécialisation des ses services de sécurité intérieure. La voie choisie est celle d'un encadrement suffisamment étroit pour limiter les externalités de cette blockchain, tout en permettant son déploiement dans les secteurs clefs de l'économie. Par ailleurs, le traitement français du Métavers se distingue par une volonté affichée d'en faire un instrument de soft power au service de la compétitivité. A ce titre, le rapport interministériel évoqué[543] sur Métavers précise que *"les métavers s'annoncent à la fois comme un marché porteur d'opportunités dont l'écosystème français pourrait se saisir, et un grand défi anthropo-technico-économique. Les métavers constituent une*

[542] E. DURKHEIM,*De la division du travail social*, Paris, Félix Alcan, 1893.
[543] A.BASDEVANT C. FRANCOIS R. RONFARD, Mission exploratoire sur les métavers, octobre 2022.

opportunité culturelle pour la France et probablement une source de créations d'emplois en tant que telle". L'usage qui en sera fait déterminera donc son acceptation par la population. Il en ira de même pour la technologie de la chaîne de blocs.

346.- L'avenir de la blockchain reste à tracer. Bien qu'elle soit née il y a près de trente ans, cette structure décentralisée n'a pas encore montré toutes ses potentialités. Cantonnée initialement à un usage purement financier en tant que fondement des crypto-monnaies, elle recèle en réalité des solutions d'amélioration du cadre global de la société. Tout dépendra donc de choix actuels, qu'ils soient individuels ou collectifs. L'influence des sources internationales sera aussi structurante afin d'harmoniser les conceptions étatiques dans un souci de réciprocité et d'interopérabilité. S'il sera impossible de parvenir à un consensus - national et international - l'adhésion du plus grand nombre permettra de rendre la blockchain plus acceptable et de réduire la défiance à son égard. Or, pour lutter contre les infractions commises contre et par la chaîne de blocs, la première étape sera de sensibiliser les citoyens - utilisateurs ou non - aux risques qu'elle induit. Une certaine hygiène numérique[544] devra être exigée afin de limiter au maximum les failles par lesquelles s'immiscent aujourd'hui les criminels. Une fois celles-ci jugulées, l'État - par le biais de ses services répressifs - devra être à la hauteur de ce défi du XXIème siècle.

[544] "Guide d'hygiène informatique", ANSSI, 2013 .

Bibliographie

I. OUVRAGES GÉNÉRAUX, TRAITÉS, MANUELS

Aristote, *Politique*, livre I, IV^e siècle av. J.-C.

B. BADIE, *La Fin des territoires*, Fayard, 1995.

N. CATELAN, *Droit pénal des affaires*.

V. CHAMPEIL-DESPLATS, *Méthodologies du droit et des sciences du droit*, Dalloz, 2014.

C. DARWIN, *L'Origine des espèces,* 1859.

F. DEBOVE, F. FALLETTI, I. PONS, *Précis de droit pénal et de procédure pénale*, Major, 2022.

H. DONNEDIEU DE VABRES, *Les principes modernes du droit pénal international*, 1928, Sirey.

J-G. DUMAS, P. LAFOURCADE, A. TICHIT et al, *Les blockchains en 50 questions. Comprendre le fonctionnement de cette technologie,* sous la direction de Paris, Dunod, « Hors collection », 2022.

E. DURKHEIM *De la division du travail social*, Paris, Félix Alcan, 1893.

E. DURKHEIM, *Les règles de la méthode sociologique* (1894), Paris, P.U.F., 14e édition, 1960.

C. FERAL-SCHUHL, *Cyberdroit*, 7^e éd., 2018, coll. Praxis, Dalloz.

C. GAU-CABÉE, *Arbitrium judicis. Jalons pour une histoire du principe de la légalité des peines*, L.G.D.J, 2007.

B. E. HARCOURT, *La société d'exposition. Désir et désobéissance à l'ère numérique,* Paris, Seuil, 2020.
S. Henry, *Droit de l'Union européenne*, Ellipses, 2020.

Hésiode *Les Travaux et les Jours.*

V. HUGO, *Les Feuilles d'automne*,1831.

X LAGARDE, *La preuve en droit* in Dominique Rousseau éd., *La Preuve* (pp. 101-124). Odile Jacob, 2003.

O. LECLERC, *Jalons prospectifs sur l'exigence de reproductibilité dans la recherche juridique,* in Mélanges en l'honneur de Pascal ANCEL, Larcier, LexisNexis, 2021.

C. LEFORT, *Le Temps présent. Écrits 1945-2005,* Belin, 2007.

A. LEPAGE, P. MAISTRE DU CHAMBON, R. SALOMON, Droit pénal des affaires, 5 e édition.

G. LEVASSEUR, *Cours de droit pénal général complémentaire,* Paris les Cours de droit 1960.

C. LOMBOIS, Droit pénal international, 2e éd., 1979, *Dalloz.*

B. PASCAL, *Pensées diverses III* – Fragment n° 31 / 85, 1678.

M. QUEMENER, *Le Droit face à la disruption numérique*, Gualino.

A. SMITH, *Recherches sur la nature et les causes de la richesse des nations,* 1776, W. Strahan and t. Cadell, Londres.

H. ROSA, *Accélération*, 2013.

II. DICTIONNAIRES, GLOSSAIRES

ABC du droit international public.

Annuaire français de droit international, volume 20, 1974.

bitFlyer.com, Glossaire “Cold storage”.

Dictionnaire Larousse, 2000.

Dictionnaire Le Robert, 2019.

Dictionnaire de droit international pénal, Genève: Graduate Institute Publications, 1998

H. MOUTOUH, *Dictionnaire du renseignement,* Perrin, 2018

France diplomatie, ministère des Affaires étrangères, « Commission rogatoire internationales ».

J. SALOMON, *Dictionnaire du droit international public*, Bruylant 2001.

G. THINES et A. LEMPEREUR, *Dictionnaire général des sciences humaine*s, Paris, Éditions universitaires, 1975

Glossaire du droit international.

Glossaire Géoconfluence, ENS Lyon, juin 2022.

III. THÈSES, MÉLANGES

K. BRISSAUD, L’influence *d’internet dans la radicalisation.* Droit. 2018.

M. DUTHOIT, *La coopération pénale au sein de l’Union européenne,* Panthéon Assas, 2010.

S. GUINCHARD, “Rapport de synthèse” in *La spécialisation des juges,* Presses de l’Université Toulouse 1 Capitole, LGDJ - Lextenso Éditions, 2012.

S. MAMMAR, *Le Bitcoin peut il être considéré comme une valeur refuge au vu de sa volatilité,* Mémoire de recherche à l'Université de Namur, 2022.

A. REUTER, *Rôle du Bitcoin sur les marchés financiers : Analyse de ses propriétés et de son potentiel rôle de valeur refuge,* Mémoire de recherche à l'Université de Namur, 2022.

L.SANTOLINI, *La stabilité économique, sociale et politique à l'ère du numérique : Exploration des options qui s'offrent aux régulateurs en matière de réglementation des crypto-monnaies,* Louvain School of Management, Université catholique de Louvain, 2019.

IV. RAPPORTS, PROPOSITIONS

ACPR, Rapport annuel 2021.

Agence nationale de sécurité des services informatique (ANSSI), *Guide des attaques par rançongiciel, tous concernés,* août 2021.

Analyse nationale des risques de blanchiment de capitaux et de financement du terrorisme en France", *Rapport du Conseil d'orientation de la lutte contre le blanchiment decapitaux et le financement du terrorisme,* septembre 2019.

Berkeley Protocol on Digital Open Source Investigations : A Practical Guide on the Effective Use of Digital Open Source and Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law, 3 janvier 2022.

A. BASDEVANT C. FRANCOIS R. RONFARD, *Mission exploratoire sur les métavers*, octobre 2022.

V. BOYER et S. KRIMI, *Rapport d'information déposé par la Commission des affaires étrangères sur la lutte contre le financement du terrorisme,* Assemblée nationale, 3 avril 2019.

Communication de la Commission relative à un plan d'action pour une politique globale de L'Union en matière de prévention du blanchiment de capitaux et du financement du terrorisme (doc. ST 7870/20), 7 mai 2020.

Conseil d'État, *Internet et les réseaux sociaux numériques,* 2 juillet 1998.

Europol, Cryptocurrencies - *Tracing the evolution of criminal finances, Europol Spotlight, 2021.*

Europol (2021), Internet Organised Crime Threat Assessment (IOCTA) 2021, Publications Office of the European Union, Luxembourg.

Euro numérique : quels enjeux pour la vie privée et la protection des données personnelles ?", CNIL, 14 février 2022.

G. DE WARREN, *Enjeux et risques des crypto-actifs,* Rapport de la Direction générale du Trésor, juin 2022.

V. FAURE-MUNTIAN, C. DE GANAY, R. LE GLEUT, rapport au de l'Office parlementaire des choix techniques et scientifiques sur *Les enjeux des blockchains*, (chaîne de bloc), 20 juin 2018.

FATF, Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, 2019.

FATF, FATF Report to the G20, 2020.

FATF, *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers,* 2021.

Fiche thématique "Protection des données personnelles", Service de l'exécution des arrêts de la Cour européenne des droits de l'homme, septembre 2022.

GAFI, *Mesures de lutte contre le blanchiment de capitaux et le financement du terrorisme,2022*.

Groupe de travail interministériel sur la lutte contre la cybercriminalité, *Rapport sur la cybercriminalité, février 2014.*

F. G'SELL F. MARTIN-BARITEAU, L'impact des blockchains sur les droits de l'homme, la démocratie et l'État de droit, Rapport rédigé pour le Conseil de l'Europe, mars 2022.

S. JOISSAINS et J. BIGOT, *Cybercriminalité : un défi à relever aux niveaux national et européen,* Rapport d'information du Sénat fait au nom de la commission des affaires européennes et de la commission des lois, déposé le 9 juillet 2020.

Interpol, *Crypto Jacking*, septembre 2020.

Lettre des sénateurs démocrates au Trésor public américain, 2 mars 2022

Lignes directrices de l'approche fondée sur les risques appliquée aux actifs virtuels et aux prestataires de services liés aux actifs virtuels, GAFI, 21 juin 2019.

Mcafee, *Rapport sur les menaces associées aux blockchain*, 2018.

Ministère de l'Intérieur et des Outre-Mer, "Cybercriminalité : l'action du ministère", Actualités 2019.

Opportunities and Challenges of New Technologies for AML/CFT, FATF, Paris, France,

Projet de déclaration sur le droit à la solidarité internationale, Haut conseil des droits de l'Homme de l'ONU, 25 avril 2017 et 19 juillet 2017.

Proposition de Règlement DU PARLEMENT EUROPÉEN ET DU CONSEIL sur les marchés de crypto-actifs, et modifiant la directive (UE) 2019/1937.

Rapport de la Banque de France, "Les dangers liés au développement des monnaies virtuelles.

Rapport d'information fait au nom de la délégation aux entreprises relatif à la cybersécurité des entreprises, par MM. Sébastien MEURANT et Rémi CARDON, Sénateurs le 10 juin 2021.

Rapport du Centre d'analyse du terrorisme sur les attentats du 13 novembre 2015, 17 octobre 2016.

Rapport final de la Commission nationale sur les attaques terroristes contre les États-Unis, 22 juillet 2004.

Rapport n° 388 (2014-2015) de M. Jean-Pierre SUEUR, fait au nom de la CE moyens de la lutte contre les réseaux djihadistes, déposé le 1er avril 2015.

Rapport d'information sur la mise en œuvre des conclusions de la mission d'information relative aux crypto-actifs, présenté par Eric WOERTH et enregistré à l'Assemblée nationale le 1er décembre 2021.

Recommendations of the 4th Global Conference on Cryptocurrencies and Criminal Finances" in *4th Global Conference on Cryptocurrencies and Criminal Finances* on 18-19 November 2020.

Report on a digital euro", BCE, octobre 2020.

Sur les chaînes de blocs (blockchains), Rapport d'information n°1501 déposé par la Mission d'information commune sur les chaînes de blocs et présenté par Mme Laure De La RAUDIÈRE et M. Jean-Michel MIS, 12 juin 2018.

TRACFIN, *Activités et analyses,* 2021.

The 2022 Crypto Crime Report, Chainalysis, 2022.

Virtual Currencies : Key Definitions and Potential AML/CFT Risks", FAFT, juin 2014.

J.-L. WARSMANN, AN, CR n°18, Prop. Loi visant à faciliter la saisie et la confiscation en matière pénale, AN n° 1255.

V. ARTICLES TIRÉS D'UNE REVUE

A. AMICELLE, "La reconstruction par association des problèmes publics : retour sur l'invention du blanchiment d'argent", *Criminologie*, *49*(1), 2016

M. Bali, "Les crypto-monnaies, une application des blockchain technologies à la monnaie" : RD. Bancaire et fin. 2016, étude 8, spéc. n° 14.

A. BRILL, L. KEENE, "Cryptocurrencies : the next generation of terrorist financing ? ", *Defence Against Terrorism Review* Vol. 6, No. 1, Spring Fall 2014.

S. BERNARD, "La montée en puissance de l'investigation cyber en gendarmerie", gendarmerie.interieur.gouv.fr, 28 janvier 2020.

H. BORDET et A. ILARI, "Cybermonnaies et terrorisme", note Université Côte d'Azur, mars 2021.

J. BOURGAIS et C. OLIVIER, "La saisie pénale des actifs numériques : une saisie virtuelle ?" Gaz. Pal, 14 février 2023, n° 5.

K. J. BOWERS, S. D JOHNSON, "Measuring the geographical displacement and diffusion of benefit effects of crime prevention activity", *J. Quant. Criminol.*, 19, 275–301, 2003.

R. CARIO, "De la victime oubliée ... à la victime sacralisée ?", *AJ Pénal 2009.*

L. DE CARBONNIÈRES, « LA *SOUVERAINETÉ PÉNALE DE L'ETAT AU XXIÈME SIÈCLE, Colloque annuel de la Société française pour le droit international*, Lille, 18, 19 et 20 mai 2017.

N. CATELAN :

- "La spécialisation des juridictions pénales", in Colloque : " Faut-il déspécialiser la procédure pénale ?" Faculté de droit de Nancy, mars 2016.

- *La blockchain au service du droit pénal* « Colloque Blockchain et droit » Université de Brasilia, avril 2019.

J. CAZALA, "Le Soft Law international entre inspiration et aspiration ». Revue interdisciplinaire d'études juridiques, 66.

H. D'AGRAIN, « Géopolitique de l'espace numérique. Quelles stratégies de sécurité ? », Futuribles, 2022/6 (N° 451), p. 21-37.

J.-G. DEGOS et J.-Y. DEGOS, "Chaînes de Ponzi et théorie des catastrophes : le point de non-retour des réalités financières", *La Revue du Financier*, mars 2017.

P. DE PREUX et D. TRAVILOVIC, "Blockchain et lutte contre le blanchiment d'argent, Le nouveau paradoxe ?", Expert Focus, 1er février 2018.

E. DEZEUZE et J. BIANCHI, “Le droit pénal des crypto-monnaies”, *Revue de Droit bancaire et financier n° 3*, mai 2020, dossier 17.

B. DOUCET et I. DE LAMINNE, “Métavers : enjeux, risques et opportunités d’une réalité en devenir”, *Regional IT Wallonie-Bruxelle*, juin 2022.

F. DOUZET. « La géopolitique pour comprendre le cyberespace ». In Hérodote 152-153, 2014.

A. El Mejri, “La pyramide de Ponzi”*, Revue de Droit bancaire et financier* n° 4, Juillet 2020, étude n° 11.

“A propos d’Europol”, Europol.europa.eu., 24 janvier 2023.

F. FABIANI, “Monnaie électronique et affaire Liberty Reserve : quelle réglementation applicable en France ?”, Village justice, 13 juin 2013.

M.FERRARI, « Art et blanchiment d’argent », *Sécurité globale*, 2016/3 (N° 7).

J. FONTANEL. Le crime international organisé et les cryptomonnaies. “ Les Géopolitiques ” de Brest, Université de Bretagne Occidentale (UBO); IMT Atlantique; ENSTA Bretagne; École navale, février 2022.

P. GERBET, Europol, CVCE.ue.

C. GHICA-LEMARCHAND, *L’interprétation de la loi pénale par le juge,* Colloque sur l’office du juge au Sénat, 29 et 30 septembre 2006.

J. GOLDSZLAGIER – A. LE TEURNIER, La lutte contre le blanchiment à l'épreuve de la territorialité des crypto-actifs, AJ Pénal, 2021.

H. JEAN-BENOIT, “La preuve par la blockchain” *in Les blockchains et les smart contracts à l'épreuve du droit*, p. 185-208, Collection du CRIDS; No. 49, 2020.

I. JEGOUZO, “Le développement progressif du principe de reconnaissance mutuelle des décisions judiciaires pénales dans l'Union européenne”, *Revue internationale de droit pénal*, 2006/1-2 (Vol. 77).

A. JOMNI, ”Le Darknet est-il une zone de non droit ?”, Sécurité globale, 2018/3 (N° 15).

L.LESSIG, Code is Law – On Liberty in Cyberspace, Harvard Magazine, janvier 2000.

A. LEJNIECE, « Les crypto-monnaies au cœur de la guerre de la Russie contre l’Ukraine », *RED*, 2022/1 (N° 4).

J. MARTINON, *Phénomènes criminels célèbres ou exotiques dans le champ des crypto-actifs*, Dalloz IP/IT, n°10, 2019.

I. MAHAMOUD, « Comprendre le fonctionnement des hawalas : pour une meilleure régulation », *Techniques Financières et Développement*, 2014/1 (N° 114).

R. MATZUTT, J. HILLER, M. HENZE, J. H. ZIEGELDORF, D. MÜLLMANN, O. HOHLFELD, K. WEHRLE, “A quantitative analysis of the impact of arbitrary blockchain content on bitcoin”, *Communication and Distributed System*s, RWTH Aachen University, Germany, 2018.

A. MELACHRINOS, C. PFISTER, “Stablecoins : le meilleur des mondes ?”, *Revue française d'économie*, 2020/4 (Vol. XXXV).

R. NOBLE, L'Interpol du xxie siècle. *Pouvoirs* 132, 2010.

P. PERROT, “Le métavers : un nouvel univers, une nouvelle criminalité !”, *Institut Europia*, novembre 2021.

Politique de sécurité : analyses du CSS, “Rançongiciels : approches nationales de protection”, No 297, Février 2022

C. POTIER, “Le procureur européen délégué, Janus judiciaire ?”, *Actu juridique, Lextenso*, 14 février 2020.

L. PROSPERI, “Le cyber, un facteur d’instabilité internationale”, https://laurentprosperi.info/fr/, 2020.

J. PROST et A. JEAN-BAPTISTE, “Les Non-fungible tokens saisis par le droit”, *Dalloz IP/IT,* 5, mai 2022

Questions à Olivier Le Guen sur la perquisition et la saisie des crypto-actifs” in Dossier : La justice pénale à l'épreuve des cryptomonnaies”, Dalloz *IP/IT,* 2019.

R. ROUMANOS, « Les promesses et les défis journalistiques de l’*Open Source Intelligence* (OSINT) », *I2D - Information, données & documents*, 2021/1 (n° 1).

M. SEGONDS, “Les métamorphoses de l'infraction de blanchiment... ou les enjeux probatoires de la lutte contre le blanchiment*” AJ Pénal 2016 n°4.*

J. SOLOMON-STRAUSS, “Terrorist Use of Virtual Currencies, Containing the Potential Threat”, *Center for New American Security*, 3 mai 2017.
M. TORELLI et G. HAAS, “Non-Fungible Token (NFT) : un outil efficace de protection des marques”, *RLDA* 2021, n° 175.

A.Y. SHEHU, “The Asian Alternative remittance System and Money Laundering”, 2003 in M. VALERI, R. FONDACARO, C. De ANGELIS et A. BARELLA, “The Use of Cryptocurrencies for Hawala in the Islamic Finance”, *European Journal of Islamic Finance,* 11 octobre 2020.

G. THIERRY, « Comment la justice travaille avec les recherches en sources ouvertes », *Dalloz actualité*, 8 juill. 2022.

“La coopération judiciaire en matière pénale”, Touteleurope.eu, 16 février 2018.

G. VIAL, O. LECLERC, E. VERGES, Preuves scientifiques et technologiques, Cahiers, Droit, Sciences et Technologies, Presses universitaires d'Aix-Marseille, 2020.

M.WEBBER, V. ELFVING, S. WEIDT et al., "The impact of hardware specifications on reaching quantum advantage in the fault tolerant regime", *AVS Quantum* Sci. **4**, 013801 (2022).

C. ZERBIB et W. O' RORKE, "NFT: chaînon manquant ou maillon faible de l'art numérique", *Propr. ind,* 2021, n° 5, étude 11

VI. ENCYCLOPÉDIE ET RÉPERTOIRES

B. AUBERT, "Entraide judiciaire : matière pénale", *Répertoire de droit international*, Dalloz, 2000.

C J. BERR, "Blanchiment de capitaux et financement du terrorisme", *Répertoire de droit commercial*, Dalloz, Janvier 2010 (actualisation : Octobre 2022).

F. Chopin, Cybercriminalité", *Répertoire de droit pénal et de procédure pénale*, Dalloz, 2020.

R. GASSIN, Fraude informatique, *Répertoire de droit pénal et de procédure pénale,* Dalloz 1995.

Y. MAYAUD, "Terrorisme - Prévention", *Répertoire de droit pénal et de procédure pénale,* Dalloz, février 2020.

VII. NOTES, JURISPRUDENCE

A. CAPRIOLI, "La nature du Bitcoin enfin précisée", note ss T. com. Nanterre, 6e ch., 26 févr. 2020, n° 2018F00466 (non publié)

TGI Lyon, 18 juin 1970.

TGI Paris, 16 décembre 1997.

TGI Paris, 25 févr. 2000.

CA Paris, 30 octobre 2002.

CA Paris, 26 septembre. 2013, n° 12/00161, Macaraja c/Crédit industriel et commercial

CA Paris, pôle 5 - ch. 15, 14 avr. 2021, n° 20/18863.

Crim. 3 août 1912 : DP 1913. 1. 439 ; S.1913. 337, note ROUX.

Crim. 21 oct. 1991, pourvoi n° 90-85.123.

Crim. 15 juin 1993, pourvoi n° 92-82.509.

Crim, 14 janvier 2009, pourvoi n° 08-82.095.

Crim. 30 sept. 2009, pourvoi n°09-80. 379.

Crim, 9 nov. 2010, inédit, pourvoi n° 10-82.918

Crim., 20 mai 2015, pourvoi n° 14-81.336.

Crim, 26 octobre 2016, pourvoi n° 15-84.552.

Crim, 28 juin 2017, pourvoi n° 16-81.113.

Crim, 4 juin 2019, pourvoi n°14-82.332.

Crim. 18 mars 2020, n° 18-86.491.

Crim., 7 septembre 2021, pourvoi n° 19-87.03.

Crim., 15 décembre 2021, pourvoi n° 21-81.864.

Cour de cassation, Assemblée plénière, 7 novembre 2022 pourvoi n° 21-83.146.

Cons.const.,16 juin 1999, décision n° 99-411 DC.

Cons.const., 10 mars 2011 décision n° 2011-625 DC.

Cons.const., 30 mars 2018 décision n° 2018-696 QPC.

CEDH 20 nov. 1989, *Kostovski c. Pays-Bas*, requête n°11454/85.

Dutch Suprem Court, J. 10/00101, Criminal Chamber, January 31, 2012.

VIII. ARTICLES EN FRANÇAIS

N. AÏT-KACIMI, “La Russie capte 120 milliards de dollars en bitcoin et cryptos”, *Les Échos*, 13 octobre 2022.

A. ALBERTINI, “Cryptomonnaies : les cyber gendarmes démantèlent une plate-forme de blanchiment”, *Le Monde*, 19 janvier 2022.

P. ANTHONIOZ, “Miner des cryptomonnaies pour gonfler son salaire, une promesse alléchante très risquée”, *Moneyvox.fr*, 8 juillet 2022.

F. BAYARD, “La blockchain, un danger pour la liberté et la vie privée ?”, *Cryptocat.fr*, 20 octobre 2020.

Binance Academy.com, “Qu'est-ce qu'une passerelle blockchain ?”, 11 novembre 2022.

Blog-wallet-crypto, “Qu’est-ce-qu’un wallet crypto ?”, 4 novembre 2021.
Bureau des affaires criminelles de la gendarmerie nationale, “Retour sur l’affaire EncroChat, ou quand les cyber-gendarmes ont hacké la messagerie chiffrée utilisée par la criminalité organisée”, 29 juillet 2020.
L. CARRIVE, “Quand la réalité virtuelle se met au service de la lutte contre les violences conjugales", Radio France, 24 janvier 2021.

G. CHAMPAU, “Second Life: un procès pour le droit de propriété virtuel », *Numerama,* 11 mai 2010.

C. CHENAIS, “Qu’est-ce qu’un mixer de Bitcoin et comment est-ce que ça fonctionne ?”, *France Crypto.fr,* 12 mai 2021.

Coin Academy.fr, “Qu’est-ce qu’une attaque par double dépense sur la blockchain ?"

Cointribune.com, “Qu’est-ce que le Byzantine General Problem”, 3 octobre 2021.

Crypto actu.com:

- “Qu’est-ce qu’une monnaie fiat?” 16 novembre 2022.
- “De l’usage de la blockchain en Chine comme outil de surveillance: un modèle exportable?”, 20 janvier 2020.
-

Cryptoast.fr:

- “Blockchain publique et blockchain privée : quelle est la différence », 29 novembre 2022.

- “Europol ferme un des plus grands mixeurs de cryptos mondiaux pour blanchiment de fonds”, 19 avril 2020.

- “Formation des forces de Police à la blockchain : entretien avec le Major Erwan Bouliou”, 30 septembre 2022.

- “Qu’est-ce que le Web3, cette version décentralisée d’Internet?”, 22 novembre 2022.

- “Stablecoin, tout savoir sur ce type de cryptomonnaie”, 9 décembre 2022.

Crypto-métaverse.info “L’Art NFT: des tableaux 3.0 cryptés et immatériels”, 9 août 2022.

*Cyber malveillance.gouv.*fr, « Attaque DDoS, que faire *? »,* 9 octobre 2019.

Cybersécurité-solutions.com, “Des réseaux de ventes de fausses crypto-monnaies démantelés en Bulgarie, en Serbie et à Chypre”, 13 janvier 2023.

M. FABRION, “Quand les groupes terroristes s’intéressent aux NFT”, *LesNumeriques.com*, 6 septembre 2022, consulté le 12 décembre 2022.

E. FERARD, “Charles Darwin : qu'est-ce que la théorie de l'évolution ?”, *Geo.fr*, 11 février 2022.

R. HOUEIX, « Les cryptomonnaies, nouvelle arme des groupes terroristes ? », *France24*, 22 août 2019.

A. GAYTE, « Do Kwon, le fondateur de la crypto Terra, est maintenant un fugitif recherché par Interpol », *Numerama*, 26 septembre 2022.

Interpol, “Élaborer la réponse internationale à apporter à la criminalité financière et à l’utilisation des cybermonnaies à des fins illicites”*,* 20 novembre 2020.

Le Big Data.fr, “Monero, tout savoir sur la monnaie préférée du Dark Web", 21 janvier 2022.

R. RAPHAËLLE et L.XI, « Bons et mauvais Chinois : Quand l’État organise la notation de ses citoyens »*, Le Monde diplomatique*, janvier 2019.

ORWL Avocats, “PSAN : Comment contester une décision du régulateur ?”, 4 mai 2021.

A. ROBINE, “Qu’est-ce qu’un PSAN ?” Captaincontrat.com, 2 novembre 2022.

F. VAIRET, “Drogue et dark web : la face sombre des crypto monnaies"*, Les Echos*, 7 juin 2021.

T. VIALLAT, “Y a-t-il une justice dans la Métaverse?”, 25 septembre 2021.

l’Usine digitale.fr, “La police a saisi 19 million d'euros sous forme de crypto actifs issus de ransomwares, 16 décembre 2021.

IX. ARTICLES EN ANGLAIS

D. BODIGER et L. ARIAS, “Millions of dollars in limbo after shuttering of digital currency site Liberty Reserve”, *TicoTimes.net*, 24 mai 2013.

J. CLOTHERTY, “Black Market Bank' Accused of Laundering $6B in Criminal Proceeds”, *abc. news*, 29 mai 2013.

Department of Justice U.S. Attorney’s Office Southern District of New York : “Former Employee Of NFT Marketplace Charged In First Ever Digital Asset Insider Trading Scheme”, 1er juin 2022.

Department of Justice, “Chief Technology Officer of Liberty Reserve Sentenced to Five Years in Prison”, 12 décembre 2014.

Department of the Treasury, “Study of the Facilitation of Money Laundering and Terror Finance Through the Trade in Works of Art”*,* février 2022.

Europol, “Policing in the metaverse : what law enforcement needs to know”, , 21 octobre 2022.

A. GREENBERG, “Meet The 'Assassination Market' Creator Who's Crowdfunding Murder With Bitcoins”, Forbes.com, 18 novembre 2013.

Interpol, “INTERPOL launches first global police Metaverse”, 20 octobre 2022.

O. KHARIF, “Crypto Terrorism Funding Is Growing More Sophisticated”, Bloomberg 17 janvier 2020.

L.H Newman, “How a Bitcoin Trail Led to a Massive Dark Web Child-Porn Site Takedown", *The Wired,* 16 octobre 2018.

C. RUTH, “Crypto hackers stole almost $2 billion in H1 2022”, *Atlas VPN.com*, 5 juillet 2022.

Wall Street Journal, “Islamic State Turns to NTFs to Spread Terror Message”, 6 septembre 2022.

X. SITES INTERNET

https://blockchainfrance.net/decouvrir-la-blockchain/c-est-quoi-la-blockchain/

https://www.blockchain.com/explorer

https://cryptoparrot.com/

https://www.cryptovantage.com/fr/guides/une-breve-histoire-de-la-cryptomonnaie/

https://www.electronicid.eu/fr/blog/post/kyc-know-your-customer-france/fr

https://journalducoin.com/bitcoin/multimillionnaires-bitcoins-perdu-acces/

https://fr.wikipedia.org/wiki/Cryptographie_asym%C3%A9trique

https://youtu.be/XbnLkc6r3yc

TABLE DES MATIÈRES

Résumé

La blockchain est une notion qui ne cesse de susciter l'attention d'une partie croissante de la communauté scientifique mais également de la société civile. Appréhendée sous l'angle économique, elle apparaît comme un formidable outil au service de la performance et de l'automatisation des tâches. Dans son approche politique, elle constitue un point d'achoppement entre États selon la conception qu'ils ont de la blockchain en général et de la crypto-monnaie en particulier - principal vecteur de cette économie 3.0. Pourtant, l'aspect criminogène de la blockchain semble avoir été occulté des débats et de la recherche au point d'en faire un impensé de cette technologie. Or, force est de constater que le perfectionnement des techniques criminelles appelle une attention accrue des acteurs de la répression. C'est pour souligner les risques que soulève la blockchain et ses émanations dans le cadre de la criminalité que ce travail de synthèse a été mené. Il aura eu pour objet, si ce ne pour effet, de mettre en lumière les liens étroits qui unissent la technologie et le crime dans son acception la plus large, afin de formuler des propositions tendant à lutter plus efficacement.

Blockchain is a concept that continues to attract the attention of a growing part of the scientific community but also of civil society. From an economic point of view, it appears as a formidable tool for performance and task automation. In its political approach, it constitutes a stumbling block between States according to the conception they have of blockchain in general and of crypto-currency in particular - the main vector of this 3.0 economy. However, the criminogenic aspect of blockchain seems to have been overlooked in debates and research to the point of making it an unthinkable aspect of this technology. However, it is clear that the improvement of criminal techniques requires increased attention from law enforcement. It is to highlight the risks that blockchain and its emanations raise in the context of crime that this synthesis work has been conducted. Its purpose, if not its effect, is to highlight the close links between technology and crime in its broadest sense, in order to formulate proposals to fight more effectively.