AUTORITÉ NATIONALE DES JEUX

Un régulateur au service d'un jeu sûr, intègre et maîtrisé



RÉPUBLIQUE FRANÇAISE

Analyse des risques de blanchiment de capitaux et de financement du terrorisme associés au secteur des Jeux à objets numériques monétisables

15/10/2026

Table des matières

SYNTHÈSE **3**

1. INTRODUCTION **4**

2. MÉTHODOLOGIE D'ÉVALUATION DU RISQUE **6**

3. ASPECTS TRANSVERSAUX À TOUTES LES OFFRES **7**

3.1. NATURE DES SERVICES PROPOSÉS AU PUBLIC PAR LES ENTREPRISES DE JONUM 7

3.2. MENACES PESANT SUR LE SECTEUR DES JONUM 8

3.3. VULNÉRABILITÉS TRANSVERSALES 9

3.3.1. Vulnérabilités liées à la nature de l'activité *10*
3.3.2. Vulnérabilités liées à la nature de l'offre *11*
3.3.3. Vulnérabilités liées aux mouvements enregistrés sur les comptes de joueur *12*
3.3.4. Vulnérabilités liées à la clientèle *12*

4. RISQUES SECTORIELS **14**

4.1. MESURES D'ATTÉNUATION 14

4.1.1. Mesures d'atténuation prévues par la règlementation relative à la LCB-FT *14*
4.1.2. Mesures d'atténuation prévues par la Loi, hors règlementation relative à la LCB-FT *15*
4.1.3. Action de supervision de l'ANJ *16*

4.2 RISQUE RÉSIDUEL 17

SYNTHÈSE

La présente analyse évalue les risques de blanchiment de capitaux et de financement du terrorisme auxquels est exposé le secteur des Jeux à objets numériques monétisables (JONUM) supervisé par l'Autorité nationale des jeux (ANJ).

Cette évaluation a été réalisée suivant une méthodologie universellement adoptée, consistant à identifier les menaces qui pèsent sur le territoire national, les vulnérabilités intrinsèques qui peuvent rendre le secteur des JONUM attractif pour les criminels et les mesures prises pour atténuer ces risques.

Cette analyse met en évidence que le secteur des JONUM peut être attractif pour des criminels désireux de blanchir des sommes potentiellement importantes. Les menaces qui pèsent sur le secteur sont avérées, tant en matière de blanchiment de capitaux que de financement du terrorisme.

Les vulnérabilités intrinsèques au secteur des JONUM expliquent cet attrait : des paiements y sont réalisés en crypto-actifs, l'offre de jeu y est disponible à distance (par internet) à toute heure et les fraudes, documentaires en particulier (puisque le client n'est pas physiquement présent au moment de l'établissement de la relation d'affaires), sont possibles. Le niveau des vulnérabilités intrinsèques du secteur pris dans son ensemble apparaît ainsi élevé.

Ces vulnérabilités font toutefois l'objet de mesures d'atténuation puisque la règlementation applicable au secteur encadre les JONUM, assujettit les entreprises qui les proposent aux obligations prévues en matière de LCB-FT par le code monétaire et financier et désigne l'ANJ en tant que superviseur, ce qui implique que cette dernière les accompagne dans l'exécution de leurs obligations et en contrôle le respect. Ces vulnérabilités ont également vocation à faire l'objet de mesures d'atténuation mises en œuvre par les entreprises de JONUM.

Le croisement des menaces et vulnérabilités résiduelles, après prise en compte des mesures d'atténuation, conduit à établir un **niveau global de risque élevé du secteur des JONUM**.

1. INTRODUCTION

1. L'approche fondée sur les risques est considérée comme le moyen le plus efficace de lutter contre le blanchiment des capitaux et le financement du terrorisme : en adoptant ce type d'approche, les autorités publiques et les autres entités participant au dispositif national de lutte contre le blanchiment de capitaux et le financement du terrorisme (ci-après, « *LCB-FT* ») s'assurent que l'intensité des mesures de prévention et d'atténuation des risques qu'elles mettent en œuvre est adaptée à leur exposition aux risques.

2. Le droit positif souligne le caractère fondamental de cette approche, qu'il incombe aux États et à leurs organes de suivre. En effet, le Groupe d'Action FInancière (GAFI[1]) recommande que les États identifient, évaluent et comprennent leurs risques de blanchiment de capitaux et de financement du terrorisme (ci-après, « *BC-FT* ») afin d'allouer les ressources de façon efficiente à leur gestion et prévention[2]. La directive du 31 mai 2024[3] rappelle également que les États membres de l'Union européenne doivent identifier, évaluer, comprendre et atténuer les risques de BC-FT auxquels ils sont exposés[4]. Enfin, les articles L. 561-4-1 et L. 561-36 du code monétaire et financier (CMF) disposent que

[1] Le Groupe d'Action Financière est un organisme intergouvernemental dont l'objectif est d'établir des normes internationales, et de développer et promouvoir les politiques nationales et internationales de lutte contre le blanchiment de capitaux, le financement du terrorisme et le financement de la prolifération des armes de destruction massive. Les recommandations du GAFI sont reconnues comme les normes internationales de référence en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme, cf. https://www.fatf-gafi.org/fr/accueil/ pour plus d'informations.

[2] Recommandation n°1 sur l'Évaluation des risques et application d'une approche fondée sur les risques : « *les pays devraient identifier, évaluer et comprendre les risques de blanchiment de capitaux et de financement du terrorisme auxquels ils sont exposés […]. Sur la base de cette évaluation, les pays devraient appliquer une approche fondée sur les risques pour s'assurer que les mesures de prévention et d'atténuation du blanchiment de capitaux et du financement du terrorisme sont à la mesure des risques identifiés. Cette approche devrait constituer le fondement essentiel d'une allocation efficiente des ressources au sein du régime de lutte contre le blanchiment de capitaux et le financement du terrorisme et de la mise en œuvre de mesures fondées sur les risques pour toutes les recommandations du GAFI. […] Les pays devraient obliger les institutions financières et les entreprises et professions non financières désignées à identifier et évaluer leurs risques de blanchiment de capitaux et de financement du terrorisme et de financement de la prolifération et à prendre des mesures efficaces pour les atténuer* ».

[3] Directive (UE) 2024/1640 du Parlement européen et du Conseil du 31 mai 2024 relative aux mécanismes à mettre en place par les États membres pour prévenir l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, modifiant la directive (UE) 2019/1937, et modifiant et abrogeant la directive (UE) 2015/849.

[4] Article 8 de la Directive (UE) 2024/1640 : « *1. Chaque État membre réalise une évaluation nationale des risques pour identifier, évaluer, comprendre et atténuer les risques de blanchiment de capitaux et de financement du terrorisme ainsi que les risques d'absence de mise en œuvre et de contournement des sanctions financières ciblées auxquels il est exposé. Il tient à jour cette évaluation des risques et la révise au moins tous les quatre ans* […] *4. Les États membres utilisent l'évaluation nationale des risques pour :*
a) améliorer leurs dispositifs de LBC/FT, en particulier en identifiant les éventuels domaines dans lesquels les entités assujetties doivent appliquer des mesures renforcées selon une approche fondée sur les risques et, s'il y a lieu, en précisant les mesures à prendre ;
b) identifier, s'il y a lieu, les secteurs ou domaines comportant un risque plus faible ou plus élevé de blanchiment de capitaux et de financement du terrorisme ;
c) évaluer les risques de blanchiment de capitaux et de financement du terrorisme associés à chaque type de personne morale établie sur leur territoire et à chaque type de construction juridique qui relève de leur droit national, ou qui est administrée sur leur territoire ou dont les trustees ou les personnes occupant une position

les personnes assujetties appliquent des mesures de vigilance adaptées aux risques qu'elles ont identifiés et que les autorités de contrôle veillent à disposer d'une bonne compréhension globale des risques de BC-FT, afin de moduler la fréquence et l'intensité de leurs contrôles. Il s'ensuit que l'élaboration d'une analyse des risques de BC-FT aux niveaux national et sectoriel est une obligation pesant sur les autorités publiques participant au dispositif national de LCB-FT. L'Analyse nationale des risques (ci-après, « *ANR* ») réalisée sous l'égide du Conseil d'Orientation de la Lutte contre le Blanchiment de capitaux et le financement du terrorisme (COLB) a été publiée en janvier 2023, elle sera actualisée courant 2026. Le présent document constitue l'Analyse sectorielle des risques (ci-après, « *ASR* ») pour le nouveau secteur des « JONUM ». Elleaura vocation, elle aussi, à être actualisée en fonction d'éléments de contexte et notamment en raison de risques émergents.

3. Les entreprises de JONUM ont la qualité de personnes assujetties à la LCB-FT en application de l'article 41, XVI, A de la Loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique[5] (ci-après, la « *Loi* »).

4. L'ANJ veille au respect par les entreprises de JONUM de leurs obligations en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme[6].

5. La présente ASR a pour objet de dresser un état des lieux des risques de BC-FT auxquels sont exposées les entreprises de JONUM (ci-après, les « *entreprises* ») dont la supervision relève de la compétence de l'ANJ. Elle présente les principales menaces en matière de BC-FT auxquelles est exposé le secteur des JONUM ainsi que les vulnérabilités qui peuvent l'affecter. Sur cette base, l'ASR, rédigée en prenant en compte l'Analyse nationale des risques qu'elle complète, présente également les mesures d'atténuation mises en place (que ces dernières soient prévues par la règlementation, découlent de l'action de supervision de l'ANJ ou encore relèvent des mesures opérationnelles et des bonnes pratiques des entreprises assujetties) ainsi qu'une cotation du risque global de chaque activité. La présente ASR permet à l'ANJ de répondre à un double objectif : d'une part, planifier ses activités de supervision en déterminant le degré d'attention à accorder aux différentes catégories d'offres proposées par les entreprises qu'elle supervise et, d'autre part, assister les entreprises dans l'évaluation des risques de BC-FT auxquels elles sont individuellement exposées.

équivalente dans une construction juridique similaire résident sur leur territoire; et avoir une compréhension de l'exposition aux risques découlant des personnes morales étrangères et constructions juridiques étrangères ;
d) décider de la répartition et de la hiérarchisation des ressources consacrées à la lutte contre le blanchiment de capitaux et le financement du terrorisme et contre l'absence de mise en œuvre et le contournement des sanctions financières ciblées ;
e) veiller à l'élaboration, pour chaque secteur ou domaine, de règles appropriées en fonction des risques de blanchiment de capitaux et de financement du terrorisme ;
f) mettre rapidement à la disposition des autorités compétentes et des entités assujetties des informations appropriées leur permettant de réaliser plus facilement leurs propres évaluations des risques de blanchiment de capitaux et de financement du terrorisme, ainsi que l'évaluation des risques d'absence de mise en œuvre et de contournement des sanctions financières ciblées visées à l'article 10 du règlement (UE) 2024/1624 ».

[5] Loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique, art. 41 XVI, A : « *Les entreprises de jeux à objets numériques monétisables sont assujetties aux obligations prévues aux sections 2 à 7 du chapitre Ier et au chapitre II du titre VI du livre V du code monétaire et financier et par les dispositions européennes directement applicables en matière de lutte contre le blanchiment des capitaux et le financement du terrorisme, y compris les règlements européens portant mesures restrictives pris en application des articles 75 ou 215 du traité sur le fonctionnement de l'Union européenne ainsi que par les dispositions prises en application du même article 215 à d'autres fins. […]* ».

[6] Loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique, art. 41 XVI, A, al.2 : « *L'Autorité nationale des jeux contrôle le respect par les entreprises des obligations mentionnées au premier alinéa du présent A* ».

6. La présente ASR est réalisée au regard de la législation aujourd'hui en vigueur et des risques actuellement identifiés. Le secteur des JONUM se caractérise par de nombreuses innovations et dans de nombreux cas par l'utilisation de chaînes de blocs (« *blockchains* ») et de crypto-actifs (dont les jetons non fongibles [« *JNF* »] et les jetons utilitaires). Si les actifs numériques et l'infrastructure *blockchain* qui leur est généralement associée constituent une innovation de rupture, ceux-ci demeurent, au-delà des interrogations qu'ils soulèvent en matière de protection des consommateurs, fortement exposés à des risques de blanchiment des capitaux et de financement du terrorisme, soulignés notamment par différentes autorités supranationales et en particulier par l'Autorité bancaire européenne[7].

2. MÉTHODOLOGIE D'ÉVALUATION DU RISQUE

7. Pour exercer une surveillance du secteur fondée sur les risques BC-FT, l'ANJ développe, documente et met à jour sa propre compréhension du risque. L'adoption d'une approche fondée sur les risques s'inscrit dans un processus d'évaluation en trois étapes : 1) identifier les risques, 2) évaluer les risques (avec une gradation en fonction de leur degré de criticité) et, enfin, 3) élaborer des stratégies pour gérer et atténuer les risques identifiés.

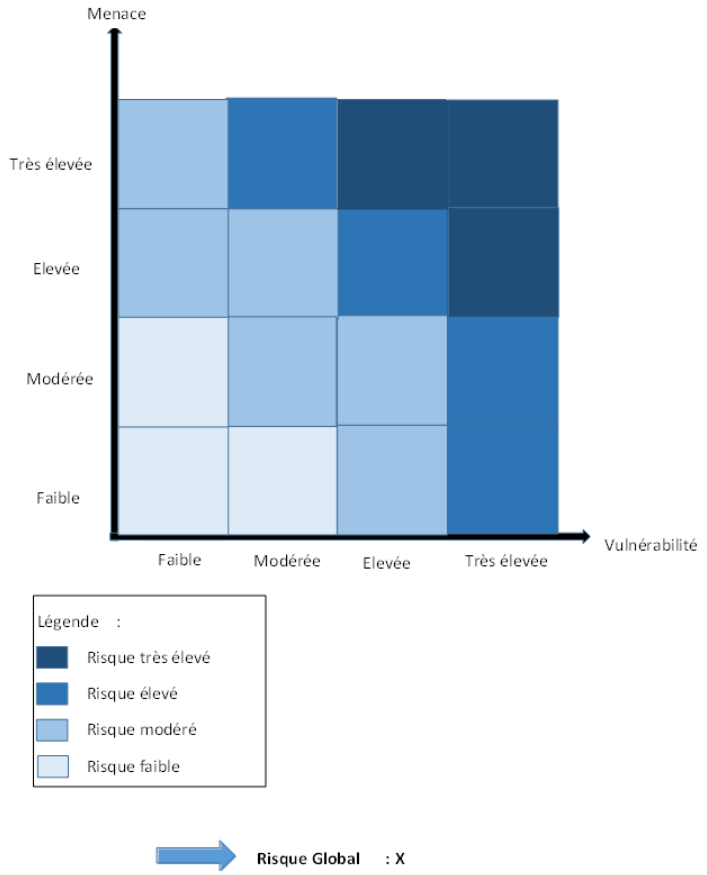
8. Le périmètre de cette ASR couvre les menaces[8] et les vulnérabilités[9] du secteur des JONUM ainsi que leurs conséquences. La méthodologie employée pour définir la cotation de chaque risque suit le principe dégagé par le GAFI du croisement entre les menaces et les vulnérabilités. Afin d'évaluer les mesures d'atténuation mises en œuvre par les entreprises, l'Autorité apprécie la solidité globale des dispositifs de LCB-FT du secteur : si l'ensemble des évaluations des risques faites par les entreprises s'avère essentiel, l'agrégation de ces évaluations par l'ANJ n'équivaut pas en soi à une évaluation sectorielle des risques, c'est pourquoi l'ANJ élabore sa propre matrice de risques selon le modèle présenté *infra*, étant précisé que figurent, sur l'axe des ordonnées, les différents niveaux de menaces (à savoir, les notations des risques inhérents[10] BC-FT) et, sur l'axe des abscisses, les vulnérabilités du secteur en tenant compte des mesures d'atténuation et de prévention des risques mises en place.

[7] Cf. communiqué commun des autorités européennes de surveillance.

[8] Une menace est une personne, un groupe de personnes, un objet ou une activité susceptible de porter préjudice au système économique, bancaire et financier. Cette notion inclut les organisations criminelles, les réseaux d'escrocs ou de fraudeurs, les réseaux de corruption, les groupes terroristes et leurs facilitateurs, leurs fonds ainsi que leurs activités passées, présentes ou futures.

[9] Les vulnérabilités comprennent les facteurs qui rendent attractives la réalisation d'une infraction et l'opération de blanchiment de capitaux ou de financement du terrorisme qui lui est liée. Elles sont inhérentes aux caractéristiques structurelles d'un pays donné et de sa place financière. Elles sont également liées aux pratiques et aux caractéristiques des produits utilisés dans un secteur d'activité donné.

[10] Les risques inhérents sont les risques de blanchiment de capitaux et de financement du terrorisme intrinsèques au secteur des JONUM, abstraction faite de la règlementation en la matière et avant l'application de tout contrôle en matière de LCB-FT ; ces risques inhérents sont associés aux caractéristiques d'une entreprise (notamment sa forme juridique, son organisation et ses parts de marché) ainsi qu'aux caractéristiques de son offre (services à sa clientèle et canal de distribution).



9. Afin d'apprécier l'exposition au risque de BC-FT du secteur des JONUM et de ses acteurs, l'ANJ prend en compte les informations relatives aux caractéristiques des services offerts et à leurs vecteurs de distribution ainsi que les constatations réalisées par les autres autorités publiques chargées de la LCB-FT. Sont ensuite appréciés les risques qui subsistent (ci-après, « *risques résiduels* ») après la mise en œuvre des mesures d'atténuation légales et opérationnelles prévues pour faire face à ces risques, le croisement des menaces et des vulnérabilités résiduelles permettant d'identifier le niveau de risque global associé à chaque segment ou produit.

3. ASPECTS TRANSVERSAUX À TOUTES LES OFFRES

10. Pour identifier et évaluer les risques associés aux activités des entreprises de JONUM, l'ANJ apprécie, dans un premier temps, la nature des services qu'elles proposent au public (**3.1**) puis dresse, dans un deuxième temps, un état des lieux de la menace au niveau national (**3.2**) avant, dans un troisième temps, d'évaluer l'attractivité du secteur des JONUM pour les personnes ou entités susceptibles de profiter de ses vulnérabilités (**3.3**).

3.1. Nature des services proposés au public par les entreprises de JONUM

11. Les articles 40 et 41 de la loi définissent les JONUM, les objets numériques monétisables (ONUM) et leur cadre de régulation : les JONUM sont des « *jeux proposés par l'intermédiaire d'un service de communication au public en ligne qui permettent l'obtention, reposant sur un mécanisme faisant appel au hasard, par des joueurs majeurs ayant consenti un sacrifice financier, d'objets numériques monétisables, à l'exclusion de l'obtention de tout gain monétaire, sous réserve que ces*

objets ne puissent être cédés à titre onéreux, directement ou indirectement par l'intermédiaire de toute personne physique ou morale, ni à l'entreprise de jeux qui les a émis, ni à une personne physique ou morale agissant de concert avec elle »[11]. Les ONUM sont « *les éléments de jeu qui confèrent aux joueurs un ou plusieurs droits associés au jeu et qui sont susceptibles d'être cédés, directement ou indirectement, à titre onéreux à des tiers* »[12], plus particulièrement les JNF et les jetons de monnaies de jeu qualifiés pour la majorité de « jetons utilitaires » au sens du Règlement (UE) 2023/1114 dit « Règlement MiCA »[13]. Les entreprises de JONUM peuvent distribuer des récompenses accessoires (qui ne sont ni des ONUM ni de la monnaie ayant cours légal) dans les conditions définies par voie réglementaire (cf. *infra*, §44). Les entreprises doivent déclarer préalablement leur offre à l'ANJ (à la différence du régime d'agrément prévu en matière de jeux d'argent et de hasard). Les catégories de jeux autorisées à titre expérimental sont limitées et sont, elles aussi, fixées par voie réglementaire. Le décret n° 2026-60 du 4 février 2026 relatif à l'expérimentation des jeux à objets numériques monétisables autorise les catégories de jeu suivantes :

- jeux d'actions et de combats avec ou contre d'autres joueurs ou avec des personnages du jeu ;
- jeux d'élevage, qui proposent aux joueurs de développer ou faire évoluer des personnages ;
- jeux de fantaisie sportive ou hippique, ayant pour support des compétitions, manifestations sportives, épreuves sportives ou épreuves hippiques réelles ;
- jeux d'aventures ou de quête ;
- jeux de gestion ou de construction ;
- jeux de courses avec ou contre d'autres joueurs ou des personnages du jeu.

12. La présente ASR a vocation à être mise à jour pour prendre en compte les spécificités des offres proposées par les entreprises de JONUM.

3.2. Menaces pesant sur le secteur des JONUM

13. Le vecteur des JONUM pourrait être utilisé par des criminels pour justifier mensongèrement l'origine de fonds déposés en vue d'être joués, ou prétendument joués, au moment de les réintégrer dans le secteur bancaire sous l'apparence de « gains ». La probabilité de survenance de ce risque est caractérisée si l'on considère l'augmentation de l'usage et de l'intérêt des investisseurs particuliers pour les actifs numériques, l'émergence de nouveaux types d'actifs numériques, de produits et de services connexes, dont font partie les JONUM ainsi qu'une maîtrise croissante par les criminels des services liés aux actifs numériques. L'ANR relève notamment que les pratiques des organisations criminelles se sophistiquent avec une appropriation croissante des nouvelles technologies cumulée avec une puissance financière considérable. Les actifs numériques viennent s'ajouter aux canaux de blanchiment déjà connus et leur usage, un temps réservé à des réseaux spécialisés dans la cybercriminalité, et est désormais largement répandu au sein de la criminalité organisée traditionnelle. Ces risques ont aussi été soulignés par la cellule nationale de renseignement financier (« TRACFIN »)[14] dans son rapport annuel consacré à l'état de la menace en matière de blanchiment de capitaux et de financement du terrorisme publié en octobre 2025[15].

---

[11] Loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique, art. 40 I, al.1er.

[12] Loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique, art. 40 I, al.2.

[13] Le règlement européen sur les marchés de crypto-actifs (*Markets in Crypto-Assets* ou « MiCA ») vise à encadrer les émissions et les services sur crypto-actifs qui ne relèvent pas des règlementations existantes en matière d'instruments financiers et de produits financiers, en créant un cadre réglementaire européen harmonisé.

[14] Pour « Traitement du Renseignement et Action contre les Circuits FINanciers clandestins ».

[15] Cf. TRACFIN, LCB-FT : état de la menace 2024-2025, p.7 où TRACFIN relève un « *recours aux cryptoactifs* [qui] *n'est désormais plus un phénomène émergent, mais ancré et répandu dans les circuits financiers illégaux. Terrain*

14. S'agissant du blanchiment de capitaux, **l'ANR identifie trois menaces criminelles majeures pesant sur le territoire national** : 1) les fraudes fiscales, sociales et douanières, 2) le trafic de stupéfiants et 3) les escroqueries et vols. De moindre volume financier mais à fort impact social, le trafic d'êtres humains, d'une part, la corruption et les atteintes à la probité, d'autre part, représentent également des sources de revenus illicites susceptibles d'être blanchis en France ou par l'intermédiaire des acteurs économiques français.

Bien que ne représentant à ce jour qu'une part encore restreinte du secteur des jeux, le secteur des actifs numériques peut donc être instrumentalisé à des fins de blanchiment de capitaux, selon des stratégies qui diffèrent en fonction de l'offre de service :

- « auto-blanchiment » à l'aide d'actifs numériques, c'est-à-dire la conversion en actifs numériques (tels que les JNF) du produit d'activités illicites comme le trafic de stupéfiants, les escroqueries ou la fraude fiscale avant reconversion en monnaie ayant cours légal. Le blanchiment peut être réalisé en utilisant des plateformes qui ne sont pas soumises à des obligations de LCB-FT ou défaillantes en matière de conformité, sur lesquelles les fraudeurs peuvent convertir des fonds illicites en actifs numériques afin de les transférer vers d'autres comptes ou de les revendre contre des monnaies ayant cours légal[16] ;
- blanchiment par l'utilisation de systèmes de compensation (espèces contre contrôle de portefeuille d'actifs numériques et *vice versa*, circuits type « *hawala* », etc.) ;
- blanchiment par « minage » en utilisant les fonds illicites à blanchir pour investir dans des installations informatiques permettant d'obtenir des crypto-actifs en récompense de la validation d'un ensemble de transactions effectuées en crypto-monnaie avant inscription sur une *blockchain*.

15. En matière de financement du terrorisme, l'État Islamique et *Al Qaïda* font toujours peser sur la France une menace élevée d'attentats, ces organisations étant principalement alimentées par des réseaux de collecteurs de fonds (parfois *via* des pseudo-organismes à but non lucratif) et par des microfinancements. Il convient de souligner ici que ces groupes terroristes ont une inclination pour l'usage de modes de financement innovants favorisant l'anonymat, tels que les cartes prépayées ou les actifs numériques. Les autorités en charge de la LCB-FT constatent une banalisation des techniques de financement du terrorisme et le contournement des sanctions économiques par le biais d'actifs numériques, dont l'usage était jusqu'à récemment réservé à des acteurs de la cybercriminalité[17]. Les autorités nationales soulignent qu'en matière de financement du terrorisme, l'utilisation des actifs numériques s'est développée, témoignant d'un accès plus aisé, dont les réseaux de financement du terrorisme peuvent profiter comme peuvent notamment l'illustrer des enquêtes menées qui identifient un recours croissant au secteur de la technologie financière.

16. Compte tenu de l'**essor de l'usage des actifs numériques** et de la **variété des JONUM**, la menace de leur utilisation à des fins criminelles est jugée **ÉLEVÉE** s'agissant tant du blanchiment de capitaux que du financement du terrorisme.

3.3. Vulnérabilités transversales

17. L'identification des vulnérabilités au niveau du territoire métropolitain, des territoires d'outre-mer et au niveau international par les autorités compétentes **est pertinente pour évaluer l'attractivité du secteur** pour les délinquants et criminels. Il convient de relever que le niveau de vulnérabilité attribué par les autorités européennes et nationales à un segment de marché ou à une

privilégié pour les escroqueries, la technologie blockchain *est aussi utilisée pour contourner les sanctions internationales et européennes, ou plus simplement pour blanchir des capitaux* ».

[16] Monnaie ayant cours légal, adossée à une banque centrale comme l'euro ou le dollar américain.

[17] Cf. Etat des lieux global des risques en matière de financement du terrorisme, GAFI, juillet 2025.

offre donnée n'est pas uniquement évalué selon le niveau d'engagement des professionnels dans la lutte contre le blanchiment de capitaux, mais dépend dans une large mesure de l'évaluation initiale de la menace sur tel ou tel segment d'un marché.

18. Il ressort de l'ANR que les crypto-actifs présentent de nombreuses vulnérabilités intrinsèques en matière de BC-FT : « *des* blockchains *ont été développées spécifiquement pour protéger l'anonymat et la non-traçabilité des transactions en recourant à des techniques cryptographiques complexes. Les utilisateurs peuvent bénéficier d'une anonymisation renforcée via certains actifs numériques (Monero ; Zcash). Les développements techniques en cours pour davantage fluidifier les transactions et en réduire le coût contribuent par ailleurs à limiter les possibilités de traçabilité (e.g. lightning network[18])* »[19]. Par ailleurs, leur nature même de crypto-actifs permet des transferts transfrontaliers**instantanés** par un simple jeu d'écriture sur la *blockchain*, la « pseudonymisation » et les multiples conversions possibles rendent leur traçabilité très difficile voire impossible dans certains cas. Pour les actifs numériques proposés par l'intermédiaire d'un service de communication au public en ligne mais ne faisant pas intervenir une *blockchain*, des transferts transfrontaliers instantanés sont également possibles, potentiellement avec encore moins de garanties en termes de sécurité et de traçage, puisqu'ils n'impliquent pas nécessairement de retranscription des informations (horodatage des transactions, références des portefeuilles d'actifs numériques impliqués etc.) sur une *blockchain* publique.

19. S'agissant de l'activité des entreprises qu'elle supervise, l'ANJ identifie des vulnérabilités liées au manque de régulation et de maturité du secteur au niveau mondial, aux variations extrêmes des prix des actifs numériques et aux risques y afférant, aux risques opérationnels et de sécurité et, enfin, aux difficultés opérationnelles et technologiques que peuvent rencontrer les autorités de poursuite dans le déroulé de leurs enquêtes.

20. Pour les besoins de la présente analyse, ces vulnérabilités ont été réparties en quatre catégories : les vulnérabilités liées à la nature de l'activité (**3.3.1**), à la nature de l'offre (**3.3.2**), aux moyens d'approvisionnement des comptes joueurs (**3.3.3**), et à la clientèle (**3.3.4**).

3.3.1. Vulnérabilités liées à la nature de l'activité

21. Les entreprises de JONUM sont *a priori* peu acculturées aux questions de LCB-FT. À l'exception de celles qui disposeraient par ailleurs d'un agrément de prestataire de services sur crypto-actifs (PSCA)[20], ces entreprises ont un niveau de maturité très faible en la matière. De manière générale, les entreprises susceptibles de proposer une offre de JONUM varient en termes de structure, de propriétés, de fonctionnement de leurs protocoles de conformité, or celles-ci exercent en France sur simple déclaration et donc sans que leur capacité de remplir durablement leurs obligations LCB-FT ait été préalablement jugée suffisamment robuste par l'ANJ, comme le prévoit au contraire le régime des agréments applicable aux opérateurs de jeux d'argent et de hasard (pour lesquels le législateur a également prévu des plans d'actions en matière de LCB-FT, afin d'accompagner leur mise en conformité).

---

[18] « *Le « lightning network » est un protocole conçu pour améliorer la scalabilité / extensibilité, tels que par la réduction des frais de transaction, l'instantanéité et la non restriction du nombre de transaction. Ce protocole fonctionne comme une deuxième couche au-dessus de Bitcoin par exemple* ». Cf. Analyse nationale des risques, ndbp n°131, p.118.

[19] Cf. Analyse nationale des risques, p.118.

[20] D'autant que parmi les PSCA, certains peuvent être des entreprises étrangères non enregistrées ni agréées auprès de l'AMF, donc non supervisées par elle, mais qui peuvent prester s'ils sont sollicités par des consommateurs sur le marché français.

3.3.2. Vulnérabilités liées à la nature de l'offre

22. Ces offres reposent sur des jeux et des choix techniques variés et très évolutifs, qui ne font pas l'objet d'une autorisation ni d'une homologation de la part de l'ANJ : choix, le cas échéant, de *blockchain* et de son niveau (« layer 1 », « layer 2 », « layer 3 »[21] etc.), de type de portefeuille d'actifs numériques, de nature des récompenses. Contrairement aux logiciels de jeu homologués par l'ANJ dans le secteur des jeux d'argent et de hasard (vérification des générateurs de nombres aléatoires etc.)[22], il n'y aura ainsi aucun contrôle du protocole des *blockchains*[23] sur lesquelles seront éventuellement « mintés »[24] les ONUM ni de contrôle au stade de la déclaration préalable des règles des JONUM.

23. En outre, le caractère mobile et immatériel des actifs numériques les rend par définition encore plus vulnérables au phénomène de BC-FT. La technologie *blockchain* permet de réaliser de multiples transactions successives, rapides, transfrontalières, potentiellement en provenance ou à destination de juridictions sans régulation, à frais réduits voire inexistants et sans tierce introduction d'un acteur de confiance soumis à de fortes exigences de LCB-FT tels que les établissements de crédits traditionnels. Cette technologie obère en grande partie les capacités d'investigation des autorités de poursuite, en raison notamment de la variété des *blockchains*, de la dispersion géographique des plates-formes de négociation de crypto-actifs (*exchanges*) et le cas échéant de leur caractère décentralisé, de la possibilité de multiplier les échanges d'actifs numériques (*swapping*), d'utiliser des AEC (*Anonymity Enhanced Cryptocurrencies*), ou encore des *mixers*[25] et des *bridges*[26].

24. La technologie sous-jacente des *blockchains* utilisée pour les actifs numériques qui y sont échangés peut comporter des risques opérationnels et des questions de sécurité spécifiques. Plusieurs émetteurs et prestataires de services d'actifs numériques, y compris les plates-formes de négociation et les fournisseurs de portefeuilles de crypto-actifs, ont ainsi été confrontés à des cyberattaques et à d'importants problèmes opérationnels. De nombreux investisseurs particuliers ont perdu leurs actifs numériques ou subi des pertes en raison de piratages/hameçonnages ou parce qu'ils ont perdu les clés privées donnant accès à leurs actifs, et d'autres ont perdu leur investissement lors d'une levée de fonds frauduleuse en crypto-actifs[27]. En résumé, l'offre de JONUM est sujette à la

[21] Ces technologies permettent de réaliser des actions non consultables depuis le niveau 1 de la *blockchain* concernée, ajoutant ainsi une couche supplémentaire de complexité pour les enquêtes légales.

[22] Conformément aux dispositions du VIII de l'article 34 de la loi n° 2010-476 du 12 mai 2010 modifiée, l'ANJ homologue les logiciels de jeu utilisés par les opérateurs de jeux agréés ou les opérateurs titulaires de droits exclusifs. L'homologation logicielle est un préalable à la mise en exploitation de tout logiciel de jeux et de paris, visant notamment à répondre à l'objectif d'intégrité, de fiabilité et de transparence des opérations de jeux prévu à l'article L. 320-3 du code de la sécurité intérieure.

[23] Le protocole d'une *blockchain* définit les règles qui régissent le réseau y compris : comment les transactions sont validées, comment les nouvelles entrées du grand livre (blocs) sont validées, la « politique monétaire » (taux d'émission de nouveaux *tokens* en récompense offerte aux « mineurs » qui valident les transactions).

[24] Opération correspondant à la création du JNF, au moment où ce dernier est enregistré pour la première fois dans la *blockchain*.

[25] Un service de *mixing* permet de regrouper et mélanger de nombreuses entrées et sorties de crypto-actifs selon un algorithme propre à chaque mixer. Les *mixers* sont des structures centralisées.

[26] Un service de *bridge* permet de déplacer des actifs numériques (tokens, *stablecoins*, JNF) d'une *blockchain* à une autre.

[27] Voir en ce sens TRACFIN, état de la menace 2024-2025, pp. 30 et 31.

quasi-entièreté des typologies intrinsèques à la cybercriminalité (rançongiciel, *cryptojacking* [28], escroquerie sentimentale, etc.).

25. Concernant spécifiquement la mécanique de jeu, les compétitions en duel ou opposant un nombre restreint de joueurs et les courses, pour celles faisant appel à l'expertise et au savoir-faire, sont exposées au risque de collusion de joueurs.

26. Enfin, les ONUM pourront être soumis à des fluctuations soudaines et extrêmes de prix puisque leurs prix dépendront principalement de la demande des investisseurs particuliers, dont certains pourraient être tentés de manipuler le « cours ». L'absence de transparence dans la méthodologie de fixation des prix (notamment lors du « *mint* » des JNF) et de l'exécution des transactions rend ces actifs vulnérables aux manipulations de marché déjà connues dans d'autres secteurs[29].

3.3.3. Vulnérabilités liées aux mouvements enregistrés sur les comptes de joueur

27. Concernant les mouvements de solde des comptes joueurs ouverts auprès d'une entreprise de JONUM, aucune limitation n'est prévue par le cadre légal, d'une part, quant au nombre et à la nature des instruments de paiement ni, d'autre part, quant à la domiciliation de ces instruments. Pour le secteur, il peut notamment s'agir de cartes bancaires, de virements depuis un compte de paiement, mais aussi de moyens de paiement tels que les portefeuilles de crypto-actifs (qu'il s'agisse de comptes de crypto-actifs ou d'adresses auto-hébergées par le joueur), et des crypto-actifs provenant potentiellement de juridictions étrangères n'ayant pas le même niveau d'exigence en matière de LCB-FT et pouvant ainsi favoriser le BC-FT. Ces derniers types de moyens de paiement souffrent notamment de vulnérabilités intrinsèques élevées liées à :

- la désintermédiation : les actifs numériques peuvent s'échanger sans intermédiaire, de pair à pair sans validation d'un tiers, de tels échanges étant d'autant plus difficiles à tracer lorsqu'ils sont réalisés sur des places de marché secondaire tels qu'*OpenSea* ou *Rarible* (actuellement exclues du périmètre de toute supervision LCB-FT en France) ;
- l'existence de portefeuilles de crypto-actifs non hébergés par un PSCA, dits « autohébergés », non contrôlés par ces derniers, permettant notamment à une personne détenant des fonds d'origine illicite de transférer des actifs numériques depuis un portefeuille hébergé par un PSCA vers un portefeuille auto-hébergé ou entre portefeuilles auto-hébergés ;
- la possibilité offerte d'utiliser des méthodes renforçant l'anonymat. Celles-ci – telles que l'utilisation de *mixers* ou d'actifs numériques renforçant l'anonymat (tels que la crypto-monnaie « *Monero* ») – compliquent le travail des enquêteurs pour tracer les fonds illicites.

3.3.4. Vulnérabilités liées à la clientèle

28. Au stade de la publication de la présente ASR, le nombre de joueurs présents sur le marché national des JONUM est incertain. Les informations relatives à l'activité économique et à la surface financière de leurs clients dont disposeront les entreprises seront *a priori* plus parcellaires que celles détenues par la majorité des autres professions assujetties au dispositif de LCB-FT, au premier rang desquelles les établissements de crédit. **La grande majorité des clients des entreprises devrait être composée de joueurs récréatifs**, dont les mises et gains moyens devraient être considérés, pour l'essentiel et dans la perspective de la LCB-FT, comme modestes. Les joueurs du secteur des JONUM peuvent être classés du point de vue de la LCB-FT en quatre catégories :

[28] Le *cryptojacking*, contraction des termes "crypto-monnaie" et "*hijacking*" ("détournement" en français), est l'acte de détourner un appareil électronique (un ordinateur, un smartphone, un objet connecté…) pour extraire des crypto-actifscontre la volonté des utilisateurs, via des sites Web ou des virus informatiques.

[29] Citons les « *wash-trading* » (transactions fictives), « *pump and dump* » (achat massif et revente subite), « auto-blanchiment » (achat-revente par la même personne).

- catégorie 1 : joueur récréatif, n'appelant *a priori* que des mesures de vigilance normales ;
- catégorie 2 : joueur qui, en raison de son activité de jeu excessive, s'avère financièrement vulnérable et donc susceptible de commettre une infraction pénale afin de financer son assuétude au jeu ;
- catégorie 3 : joueur disposant de fonds provenant d'activités potentiellement illégales utilisés à des fins récréatives ;
- catégorie 4 : joueur n'ayant pas un comportement ludique, disposant de fonds potentiellement d'origine illicite et motivé par une justification mensongère de ceux-ci.

29. Les transactions sur les *blockchains* sont pseudonymisées, ce qui signifie que les utilisateurs ne sont identifiés que par des adresses de portefeuilles, qu'il peut s'avérer difficile de rattacher aux personnes physiques bénéficiaires des transactions. Le développement d'innovations évoquées *supra* liées à la *blockchain* (cf. §18) renforce encore davantage la capacité d'anonymisation des transactions. Par ailleurs, plus l'écosystème *blockchain* se développe, plus le risque de blanchiment croît car, d'une part, les flux sont plus nombreux et, d'autre part, les sorties du « monde crypto », qui constituent des points de contrôle, sont de moins en moins nécessaires.

30. Les modalités d'ouverture, de gestion et de clôture des comptes joueurs sont précisées par décret. Il est notamment prévu par le décret que les joueurs fournissent aux entreprises les informations et documents permettant de vérifier leur identité, un compte joueur ne pouvant en principe pas être ouvert avant la vérification de l'identité et de la majorité de la personne qui en demande l'ouverture. Alors que la possibilité n'avait initialement pas été envisagée par le législateur en matière de JONUM, le décret prévoit également, d'une part, que si à l'issue d'un délai de trente jours à compter de la demande d'ouverture d'un compte joueur, l'entreprise n'a pas pu vérifier l'identité du demandeur, elle refuse l'ouverture du compte et, d'autre part, que l'entreprise peut, dans l'attente des vérifications de l'identité du joueur, proposer à ce dernier une activité de JONUM.

31. Ainsi, les vulnérabilités intrinsèques du secteur des JONUM peuvent être considérées comme **ÉLEVÉES**, tant en ce qui concerne le blanchiment de capitaux que le financement du terrorisme.

4. RISQUES SECTORIELS

32. Le secteur des JONUM est marqué par une grande hétérogénéité caractérisée par la présence d'entreprises exerçant sur des marchés différents, revêtant des formes juridiques distinctes, qui présentent un poids économique variable ainsi qu'une maturité relative en matière de LCBFT, et sont installées pour certaines dans d'autres États membres de l'Union européenne ou des pays tiers.

33. Les caractéristiques propres à chaque entreprise ou offre peuvent être exploitées et conduire à des tentatives de détournement des dispositifs à des fins de blanchiment de capitaux ou de financement du terrorisme. Face à cette menace, des mesures d'atténuation et de gestion de ces risques existent, qui sont de trois ordres (**4.1**), en considération desquelles il est possible d'évaluer, par la suite, le risque résiduel (**4.2**).

4.1. Mesures d'atténuation

34. Les mesures d'atténuation sont de trois ordres, à savoir celles prévues par le droit commun (***4.1.1.***), celles mises en place par les textes extérieurs à la réglementation propre à la LCB-FT (***4.1.2.***) et, enfin, celles liées à la supervision des entreprises par l'ANJ (***4.1.3.***).

4.1.1. Mesures d'atténuation prévues par la réglementation relative à la LCB-FT

35. La France fait partie des premiers pays au monde à s'être doté d'un cadre législatif et réglementaire *ad hoc* complet dans le domaine des actifs numériques, prévoyant l'assujettissement des acteurs à l'ensemble des règles en matière de LCB-FT avant même la transposition de la 5ème directive européenne LCB-FT. La réglementation française visant à prévenir le blanchiment des capitaux et le financement du terrorisme prévoit une série de mesures d'atténuation des risques portant, d'une part, sur la qualité des personnes autorisées à offrir des JONUM (4.1.1.1.) et, d'autre part, sur le périmètre des instruments de paiement autorisés (4.1.1.2.).

4.1.1.1. Mesures d'atténuation relatives aux personnes autorisées à offrir des JONUM

36. Les entreprises de JONUM ont été assujetties au dispositif LCB-FT 18 mois après la promulgation de la Loi (soit depuis le 24 novembre 2025). Ainsi, les entreprises doivent identifier et comprendre les risques auxquels elles sont exposées, allouer des moyens humains et matériels adaptés afin de les atténuer ou les gérer, déclarer au service Tracfin les opérations sur lesquelles persiste un doute et participer à la lutte contre le financement du terrorisme en gelant les fonds des personnes reprises sur les listes de sanctions financières ciblées.

4.1.1.2. Mesures d'atténuation relatives aux opérations financières

37. Le droit français interdit l'acquisition d'actifs numériques au moyen de « monnaie électronique » (*i.e.* faisant intervenir des supports de paiement prépayés anonymes comme les cartes bancaires prépayées) afin de lutter contre l'anonymat[30].

38. Certains criminels ont recours à des méthodes renforçant l'anonymat. Celles-ci, telles que l'utilisation de *mixers* ou d'actifs virtuels renforçant l'anonymat, complexifient le travail des enquêteurs pour tracer les fonds illicites. Toutefois, de nouvelles évolutions législatives visent à réduire leur utilisation, en particulier l'article 7 de la loi n° 2025-532 du 13 juin 2025 visant à sortir la France du piège du narcotrafic, qui intègre à l'article 324-1-1 du code pénal le recours à des outils d'anonymisation et d'opacification de transactions en crypto-actifs comme constituant un facteur de présomption de blanchiment.

[30] Article R. 561-16-1, 1° du CMF depuis sa modification par le décret n° 2021-387 du 2 avril 2021 relatif à la lutte contre l'anonymat des actifs virtuels et renforçant le dispositif national de LCB-FT.

39. Enfin, deux dispositions ont été prises pour mieux encadrer l'utilisation des cartes de paiement prépayées depuis la loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement :

- plafonnement des paramètres d'utilisation des cartes prépayées, même non-anonymes : le montant maximal stockable sur une carte prépayée et les montants de chargement, de remboursement et de retraits en espèces ou en monnaie électronique à partir d'une carte bancaire prépayée « *anonyme* » sont plafonnés à des niveaux fixés par décret ;
- obligation pour les établissements de monnaie électronique de conserver pendant cinq ans les informations clients : les émetteurs de monnaie électronique doivent recueillir et conserver pendant cinq ans les informations relatives à l'activation, au chargement et à l'utilisation de la monnaie électronique au moyen d'un support physique.

4.1.2. Mesures d'atténuation prévues par la Loi, hors réglementation relative à la LCB-FT

40. Afin d'assurer le développement de l'économie des JONUM dans un cadre protecteur, le législateur a prévu de les autoriser, à titre expérimental et pour une durée de trois ans à compter de la promulgation de la Loi. Le cadre prévoit le régime de la déclaration administrative (4.1.2.1.), une limitation du périmètre de l'offre (4.1.2.2.), un plafonnement des récompenses accessoires (4.1.2.3.) ainsi que des mesures de lutte contre la fraude à l'identité et la fraude documentaire (4.1.2.4).

4.1.2.1. Principe général de déclaration préalable d'activité

41. L'entreprise souhaitant proposer au public une offre de JONUM doit préalablement la déclarer à l'ANJ selon des modalités fixées par cette dernière[31]. De la même manière, l'entreprise, qui doit être établie soit dans un État membre de l'Union européenne, soit dans un autre État partie à l'accord sur l'Espace économique européen ayant conclu avec la France une convention contenant une clause d'assistance administrative en vue de lutter contre la fraude et l'évasion fiscales[32], doit l'informer de toute modification substantielle de cette offre[33].

4.1.2.2. Limitation et contrôle de l'offre

42. L'offre de JONUM est encadrée et contrôlée afin de prévenir les activités frauduleuses ou criminelles ainsi que le blanchiment de capitaux et le financement du terrorisme. Les catégories de jeux autorisées sont limitativement énumérées dans une liste fixée par décret (cf. *supra*, §11).

43. En outre, la participation à un jeu à objets numériques monétisables est subordonnée à la création, à la demande expresse du joueur, d'un compte joueur. L'entreprise ne peut ouvrir qu'un seul compte par joueur[34].

4.1.2.3. Nature des récompenses et plafonnement des récompenses accessoires

44. Seuls des ONUM peuvent être gagnés à titre principal. À titre accessoire, des récompenses en nature et certaines catégories de crypto-actifs peuvent néanmoins être obtenues[35]. En raison des

---

[31] Décision n° 2026-026 du 12 février 2026 relative aux modalités de dépôt et au contenu du dossier de déclaration préalable des entreprises de jeux à objets numériques monétisables : https://anj.fr/sites/default/files/2026-02/D%C3%A9cision%20n%C2%B02026-026_JONUM_DossierD%C3%A9clarationPr%C3%A9alable.pdf

[32] Loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique, art. 41 I, D.

[33] Loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique, art. 41 I, C, al.2.

[34] Loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique, art. 41 III.

[35] Décret n° 2026-60 du 4 février 2026 relatif à l'expérimentation des jeux à objets numériques monétisables, art.3 : « *Dans les jeux à objets numériques monétisables, est autorisée à titre expérimental l'attribution à titre accessoire des récompenses suivantes :*
1° Les récompenses en nature ;

vulnérabilités spécifiques inhérentes aux crypto-actifs (cf. *supra*, §18), le montant maximal pouvant être annuellement distribué avec ce type de récompense est plafonné par décret[36].

4.1.2.4. Mesures de lutte contre la fraude à l'identité

45. Considérant la vulnérabilité représentée par les relations d'affaires à distance, et dans un objectif d'efficacité en matière de lutte contre la fraude documentaire, la Loi prévoit que les entreprises mettent « *en œuvre tout moyen utile afin de procéder* » au contrôle d'identité des joueurs[37].

4.1.3. Action de supervision de l'ANJ

46. L'ANJ est désignée comme étant l'autorité de contrôle et de supervision[38] du secteur des JONUM. Elle évalue les risques ainsi que les résultats des actions menées par les entreprises en matière de LCB-FT et peut leur adresser des prescriptions à ce sujet[39]. Elle adapte de manière proportionnée les modalités, l'intensité et la fréquence de ses contrôles sur pièces et sur place en fonction des risques identifiés[40]. **L'Autorité accompagne** (4.1.3.1.) **et contrôle** (4.1.3.2.) **les entreprises assujetties aux obligations en matière de LCB-FT**. En outre, elle **lutte contre l'offre illégale** (4.1.3.3.).

4.1.3.1 Action de conformité

47. Répondant en cela aux recommandations du GAFI[41], l'ANJ accompagne la mise en conformité des entreprises, notamment en diffusant – avec ses partenaires privilégiés que sont la Direction générale du Trésor et TRACFIN – une information continue afin qu'elles disposent d'une compréhension adaptée et évolutive de leurs obligations en matière de LCB-FT. À cet effet, l'ANJ met à leur disposition des documents (guide pratique[42], analyse sectorielle des risques) et organise des actions de sensibilisation auprès d'elles, notamment en cas d'évolution de la réglementation ou de survenance d'un nouveau risque.

2° Les crypto-actifs entrant dans le champ d'application du règlement (UE) 2023/1114 du Parlement européen et du Conseil du 31 mai 2023 sur les marchés de crypto-actifs, et modifiant les règles (UE) n° 1093/2010 et (UE) n° 1095/2010 et les directives 2013/36/UE et (UE) 2019/1937 et autres qu'un jeton se référant à un ou des actifs au sens de l'article 3, paragraphe 1, point 6 de ce règlement, qu'un jeton de monnaie électronique au sens de l'article 3, paragraphe 1, point 7 de ce règlement ou qu'un jeton utilitaire au sens de l'article 3, paragraphe 1, point 9 de ce règlement. »

[36] Décret n° 2026-60 du 4 février 2026 relatif à l'expérimentation des jeux à objets numériques monétisables, art. 4 : « *La valeur totale des récompenses en nature mentionnées au 1° de l'article 3 ne dépasse pas 1 000 euros par année civile, par joueur et par jeu. La valeur totale des récompenses distribuées à l'ensemble des participants à un même jeu, au cours d'une année civile, sous la forme mentionnée au 2° de l'article 3 ne représente pas plus de 20 % du chiffre d'affaires issu de ce jeu au cours de cette même année civile, et dans la limite d'un montant annuel de 25 000 euros par joueur pour ce jeu* ».

[37] Loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique, art. 41 III.

[38] Loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique, art. 41 XVI, A, al.2.

[39] Loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique, art. 41 XVI, A, al.3.

[40] Loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique, art. 41 XVI, A, al.4.

[41] Recommandation 34 - Lignes directrices et retour d'informations des Normes internationales sur la lutte contre le blanchiment de capitaux et le financement du terrorisme - Les Recommandations du GAFI, p.27 : « *Les autorités compétentes, les autorités de contrôle et les organismes d'autorégulation devraient établir des lignes directrices et assurer un retour d'informations qui aideront les institutions financières et les entreprises et professions non financières désignées dans l'application des mesures nationales de LCB/FT, et, en particulier, à détecter et déclarer les opérations suspectes* ».

[42] Guide pratique des obligations LCB-FT pour les entreprises de JONUM, consultable ici.

4.1.3.2. Action de contrôle

48. L'ANJ élabore et met régulièrement à jour son analyse des risques de blanchiment de capitaux et de financement du terrorisme applicable au secteur, sur la base de laquelle elle oriente son action de contrôle de l'ensemble des entreprises déclarées. En vue d'assurer ce contrôle, le V de l'article 41 de la Loi prévoit que les entreprises doivent mettre à la disposition permanente de l'ANJ les données relatives aux joueurs, aux événements de jeu et aux opérations financières associées[43]. L'ANJ utilise ces informations afin notamment de s'assurer que les entreprises respectent leurs obligations en matière de LCB-FT. La Loi confère également à l'Autorité la faculté d'effectuer des contrôles sur pièces et sur place[44] et de mettre en demeure les entreprises qui manqueraient à leurs obligations légales, préalablement à une saisine de la Commission Nationale des Sanctions (CNS) sur le fondement des manquements constatés : tout manquement peut donner lieu aux sanctions prévues à l'article L. 561-40 du code monétaire et financier (à l'exception de celle prévue au 4°)[45].

4.1.3.3. Lutte contre l'offre illégale

49. L'ANJ lutte contre l'offre illégale de JONUM, sans préjudice de son action de lutte contre les offres illégales de jeux d'argent et de hasard, telles que les offres de jeu de casino en ligne[46]. L'ANJ **lutte** également **contre la publicité en faveur de l'offre illégale de JONUM**[47].

50. En dépit de ces mesures d'atténuation, la vulnérabilité résiduelle du secteur des JONUM demeure **ÉLEVÉE**.

4.2 Risque résiduel

51. L'exposition au risque dépend de la menace identifiée, de la nature et de l'étendue de l'offre, de son canal de distribution et des moyens de paiement utilisés. Le risque résiduel est évalué après l'application aux risques inhérents au secteur concerné des mesures d'atténuation législatives et opérationnelles, et des actions de supervision de l'Autorité.

52. Le croisement des menaces et des vulnérabilités résiduelles, malgré la prise en compte des mesures d'atténuation, conduit à retenir un niveau de **risque global ÉLEVÉ du secteur des JONUM.**

[43] Loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique, art. 41 V, al.1.

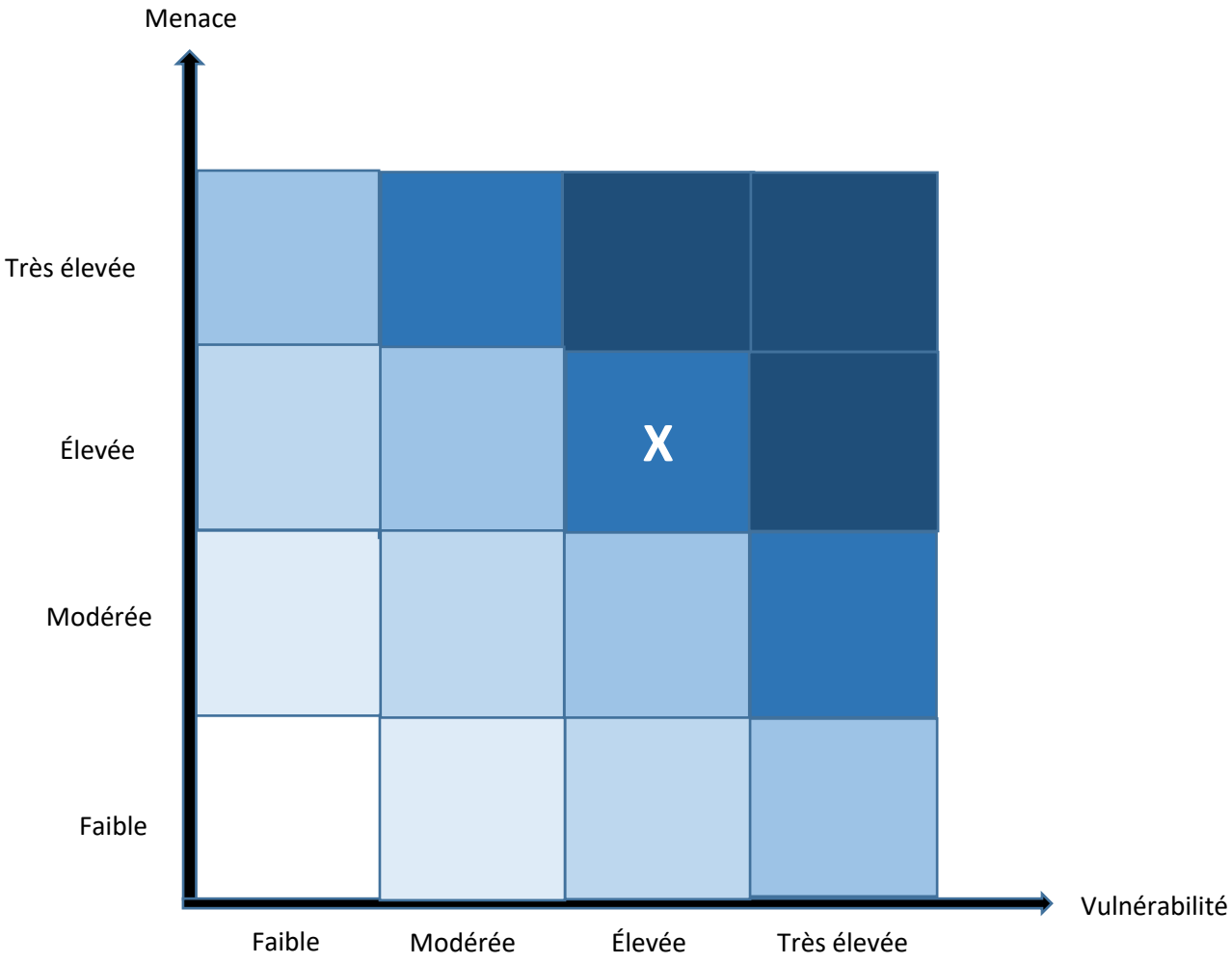
[44] Loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique, art. 41 XVI, A, al.4.

[45] Loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique, art. 41 XVI, A, al.5.

[46] Loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique, art. 41 XVII.

[47] Loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique, art. 41 XXVII et XXVIII.

Matrice de risques du secteur JONUM



Légende :

- Risque très élevé
- Risque élevé
- Risque modéré
- Risque faible

➡ **Risque global : ÉLEVÉ**