

SÉCURITÉ

#41

MARS/2024



FINANCIÈRE



PRÉSIDENT DE L'ACADÉMIE
DES SCIENCES DE RUSSIE

**GUENNADI
KRASNIKOV:**

« Nous assistons au
changement du monde qui nous
entourne grâce au progrès
scientifique. La sensibilisation de
l'information concernant
l'introduction de nouvelles
technologies, l'expérience de nos
développeurs et chercheurs jouent
un rôle très important »

DISCOURS DE BIENVENUE



YOURI TCHIKHANTCHINE

Directeur du Service fédéral de surveillance financière
Directeur du comité éditorial



CHERS LECTEURS!

Aujourd'hui, il est impossible d'imaginer le monde sans hautes technologies. Elles existent dans presque tous les domaines de la vie et font partie de nos activités quotidiennes. La technologie financière nous permet de faire un achat en un seul clic, sans aller au magasin, transférer de l'argent, payer pour les services, obtenir un prêt. C'est pratique et cela fait gagner du temps.

La tendance à la numérisation a également eu un impact direct sur les activités des autorités publiques. Comme la plupart des autres agences, Rosfinmonitoring (Service fédéral de surveillance financière) utilise plusieurs outils informatiques dans son travail.

Par exemple, notre Service collabore avec les entités du système de lutte contre le blanchiment d'argent via le compte personnel. Chaque jour nous recevons environ un million de messages de leur part et leur donnons un feedback en quelques heures suite à la réception. Il est évidemment impossible de traiter manuellement une telle quantité d'informations.

Mais il faut bien comprendre que ces technologies ont été créées par des personnes. L'intelligence artificielle, quelles que soient ses capacités, n'est qu'un assistant dans la résolution de problèmes complexes. C'est toujours un être humain qui prend la décision.

Avec le développement des hautes technologies, les risques de leur utilisation à des fins illégales ont également considérablement augmenté. L'IA et d'autres solutions informatiques ont été mise en service des malfaiteurs qui les utilisent pour le détournement de fonds, le blanchiment d'argent, le financement du terrorisme, le trafic de stupéfiants, le trafic d'armes et d'autres infractions. En même temps, la cybercriminalité est devenue transnationale.

C'est pourquoi il est si important aujourd'hui d'unir les efforts de la communauté internationale, des autorités publiques, du secteur privé et de la société civile dans la lutte contre les nouveaux défis et les nouvelles menaces.

Cette revue couvre les pratiques d'utilisation des outils numériques et de l'intelligence artificielle dans le travail des autorités publiques et des banques en Russie et à l'étranger, certains aspects de la réglementation du marché des services financiers, l'expérience en matière de détection et de répression des infractions commises à l'aide de hautes technologies et dans le cyberspace. Elle parle aussi des questions actuelles de la sécurité de l'information, ainsi que de l'utilisation des cryptomonnaies.

Nous invitons les lecteurs à s'immerger dans le monde de la haute technologie et à réfléchir de nouveau sur son rôle dans notre vie.



CONTENU

- 6 GENNADIY KRASNIKOV**
Nous souhaitons la bienvenue
aux lecteurs du journal
« Sécurité financière »

Hautes technologies de la sécurité financière

- 8 ANTON LISSITSYN**
Lutte contre le blanchiment
de capitaux et le financement
du terrorisme dans le monde
numérique : le défi de notre
époque
- 11 M. KECHAV ANANDE,
MME M. CHANMOUGA PRIYA**
Développement de la
technologie financière en Inde :
la politique visant à stimuler
l'innovation, assurer la sécurité
financière et à lutter contre la
cybercriminalité

- 15 YOURI KOROTKI :**
« La surveillance financière
est une sorte de tomographie
financière »

- 19 OTABEK RAKHMANOV**
Réglementation du marché
des technologies financières
dans le contexte de LBC/FT :
l'expérience de l'Ouzbékistan

- 24 VICTORIA KAPARTCHOUK,
YANA BAÏRATCHNAÏA,
ALEXANDRE KOURIANOV**
Utilisation des technologies
numériques dans la
surveillance et l'augmentation
du niveau de connaissances
des organisations
responsables

- 31 DINARA MOUSSINA**
Registre des bénéficiaires
effectifs. Expérience du
Kazakhstan

Le présent et le futur de l'intelligence artificielle et des technologies financières

- 35 SVETLANA ORLOVA :**
« Les produits et solutions
numériques sont des étapes
décisives vers le développement
de l'audit des finances
publiques »



- 11 M. KECHAV ANANDE, MME M. CHANMOUGA PRIYA**
Développement de la technologie financière en Inde : la
politique visant à stimuler l'innovation, assurer la sécurité
financière et à lutter contre la cybercriminalité

15

- YOURI KOROTKI :**
« La surveillance
financière est
une sorte de
tomographie
financière »



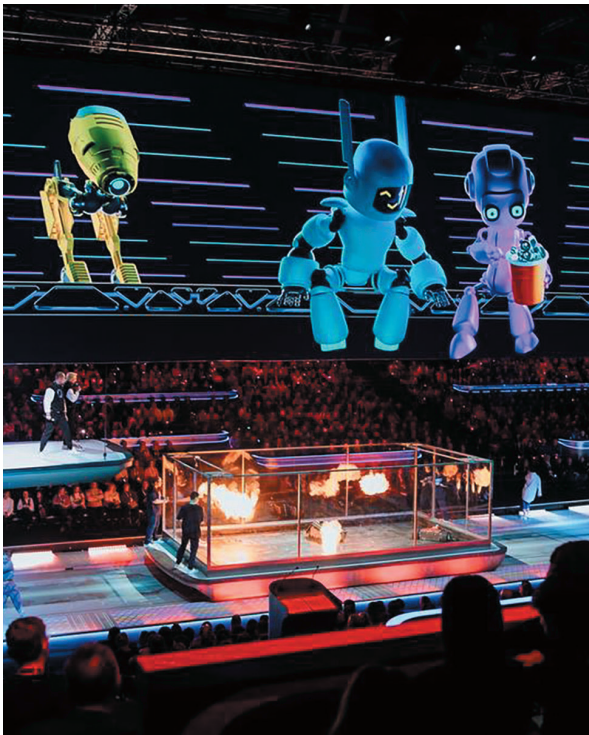
35

- SVETLANA ORLOVA :**
« Les produits et
solutions numériques
sont des étapes décisives
vers le développement
de l'audit des finances
publiques »





68 **OLGA TISENE**
Réglementation juridique de la circulation des actifs virtuels et de la lutte contre leur utilisation à des fins LBC/FT des pays EAG



- 39 VICTOR DOSTOV**
L'intelligence artificielle dans la finance et son impact sur certains aspects de la LBC/FT
- 43 MIKHAÏL PRONINE**
Application de l'intelligence artificielle pour la surveillance financière
- 46 ALEXEÏ GUELETA :**
« Le marché de la technologie financière de Russie est un des plus innovants et avancés dans le monde entier »

Détection et lutte contre la cybercriminalité

- 50 BOGDAN CHABLYA**
La lutte contre les « mules financières » et les opérations P2P à haut risque est une priorité de la surveillance financière
- 53 VADIM OUVAROV**
Sécurité de l'information du marché financier : question de la lutte contre la cyberfraude dans les transferts de fonds
- 57 ANTON RASTACHTENOV**
Restriction préalable de l'accès à des informations sur Internet dont la diffusion est interdite sur le territoire de la Fédération de Russie
- 60 ROMAN MOUKHLYNOV**
Les dernières tendances sur le marché des fournisseurs illégaux de services financiers
- 63 OLEG KIPKAÏEV**
L'utilisation des technologies numériques dans la collecte, le traitement et la généralisation des données informatiques et analytique ainsi que d'autres données utilisées dans les activités du parquet, par exemple dans le cadre des fonctionnalités du système d'information et d'analyse « Bureau électronique du procureur »

Crypto-monnaie : à la recherche de solutions

- 68 OLGA TISENE**
Réglementation juridique de la circulation des actifs virtuels et de la lutte contre leur utilisation à des fins LBC/FT dans des pays de l'EAG
- 73 DMITRI MATCHIKHINE**
Enquêtes LBC dans l'industrie Web-3
- 77 SEAN MOUNIR**
Travail avec les actifs numériques : cryptomonnaie, NFT et sécurité financière

Tribune des jeunes

- 80 SOFIA ROUDKOVITCH**
La nécessité d'une réglementation juridique des prestataires de services d'actifs virtuels à des fins de LBC/FT dans tous les pays du monde

Actualités du système anti-blanchiment

- 84** « Jeux de l'avenir ». Les gagnants du tournoi « la coupe des quatre continents » ont visité Kazan
- 85** La tenue de la première réunion en format élargi du Conseil des BRICS sur la lutte contre le blanchiment de capitaux et le financement du terrorisme
- 85** Les problèmes de sécurité financière ont été discutés au Festival mondial de la jeunesse

84 « JEUX DE L'AVENIR ». LES GAGNANTS DU TOURNOI « LA COUPE DES QUATRE CONTINENTS » ONT VISITÉ KAZAN

NOUS SOUHAITONS LA BIENVENUE AUX LECTEURS DU JOURNAL « SÉCURITÉ FINANCIÈRE »



GENNADIY KRASNIKOV,

Président de l'Académie des sciences de Russie
Académicien de l'Académie des sciences de Russie



CHERS LECTEURS,

Cette année, l'Académie des sciences de Russie fête ses 300 ans depuis sa fondation. En célébrant cet anniversaire important, nous nous souvenons non seulement du passé glorieux de la science nationale, mais nous nous tournons également vers l'avenir. Nos scientifiques travaillent sur des tâches liées au renforcement de la souveraineté scientifique et technologique de la Russie, ils parviennent à des résultats importants dans les domaines scientifiques les plus avancés.

Il faut qu'aujourd'hui nous assistons tous au changement du monde qui nous entoure par le progrès scientifique. L'introduction de nouvelles technologies, l'application de l'expérience de nos développeurs et chercheurs sont considérables.

À cet égard, il est très important que le journal « Sécurité financière

» ne s'adresse pas uniquement à des spécialistes dans ce domaine particulier. Il permet également à un large éventail de lecteurs de se familiariser avec les sujets complexes de la cybersécurité, d'apprendre les perspectives de l'intelligence artificielle dans la finance et les risques de sa mise en application généralisée.

J'espère que les lecteurs trouveront sur les pages de cette publication des articles rédigés par d'éminents chercheurs nationaux et étrangers, des experts et des représentants des autorités publiques, et qu'ils pourront en apprendre davantage sur la manière dont les processus de numérisation de l'économie et de la finance continueront d'évoluer à l'avenir.

Je vous présente tous mes meilleurs vœux de santé, de nouveaux succès éclatants et, bien sûr, le bonheur.





HAUTES TECHNOLOGIES DE LA SÉCURITÉ FINANCIÈRE

8 ANTON LISSITSYN

Lutte contre le blanchiment de capitaux et le financement du terrorisme dans le monde numérique : le défi de notre époque

11 M. KEHAV ANANDE, MME M. CHANMOUGA PRIYA

Développement de la technologie financière en Inde : la politique visant à stimuler l'innovation, assurer la sécurité financière et à lutter contre la cybercriminalité

15 YOURI KOROTKI :

«La surveillance financière est une sorte de tomographie financière»

19 OTABEK RAKHMANOV

Réglementation du marché des technologies financières dans le contexte de LBC/FT : l'expérience de l'Ouzbékistan

24 VICTORIA KAPARTCHOUK, YANA BAÏRATCHNAÏA, ALEXANDRE KOURIANOV

Utilisation des technologies numériques dans la surveillance et l'augmentation du niveau de connaissances des organisations responsables

31 DINARA MOUSSINA

Registre des bénéficiaires effectifs. Expérience du Kazakhstan

LUTTE CONTRE LE BLANCHIMENT DE CAPITAUX ET LE FINANCEMENT DU TERRORISME DANS LE MONDE NUMÉRIQUE : LE DÉFI DE NOTRE ÉPOQUE

La numérisation de tous les processus de la société devient de plus en plus importante dans le monde moderne, apportant à la fois de nouvelles opportunités et de nouveaux défis dans diverses industries et secteurs de l'économie. La croissance et le développement des technologies numériques telles que l'Internet, les applications mobiles, l'informatique en nuage, les données massives et l'intelligence artificielle entraînent des changements dans la vie des citoyens, dans la manière de travailler et d'interagir au sein des entreprises ainsi que dans le fonctionnement du secteur public



ANTON LISSITSYN,

Directeur adjoint du Service fédéral de surveillance financière

Les finances subissent également des changements importants sous l'influence de la technologie numérique. Les services bancaires en ligne, les paiements mobiles et les portefeuilles numériques simplifient et accélèrent les opérations bancaires et les paiements, tandis que la technologie blockchain et les crypto-monnaies offrent de nouvelles opportunités.

L'innovation et la transformation numérique deviennent des facteurs clés pour le développement des pays dans le cadre de l'économie numérique, contribuant à la création de nouvelles industries et de nouveaux emplois, à l'augmentation de la productivité et à une meilleure qualité de vie. L'utilisation des technologies numériques dans l'administration publique permet de simplifier

et d'automatiser les processus, d'améliorer l'accessibilité des services publics pour les citoyens, d'améliorer l'efficacité et la transparence du travail des autorités publiques et de s'adapter aux nouvelles conditions.

L'intelligence artificielle et l'automatisation ont un énorme potentiel pour améliorer les processus d'affaires et l'efficacité de l'économie numérique. L'IA peut aider à automatiser les tâches de routine, à analyser de grands ensembles de données, à prendre des décisions basées sur des algorithmes et à améliorer les performances, ce qui donne de nouvelles possibilités en matière d'analyse de données et de développement de systèmes intelligents.

En ce qui concerne la numérisation des mécanismes du Service fédéral de surveillance financière, il convient de noter que le concept de développement du Système d'information unifié de Rosfinmonitoring prévoit la mise en œuvre d'un certain nombre de domaines où l'utilisation de mécanismes d'IA est justifiée et devrait assurer une augmentation de la productivité des employés.

Les données accumulées dans le système d'information du Service depuis sa fondation représentent une quantité importante d'informations nécessaires à la mise en œuvre d'activités analytiques.

Souvent, les informations obtenues à partir de sources externes multiples et hétérogènes sont présentées d'une manière non structurée et non-formalisée, ce qui entraîne un traitement ou un ajout supplémentaire.

Lors du traitement de ces informations, leur marquage est d'une importance primordiale, car il permet d'identifier les entités commerciales pour la détection ultérieure de signes d'activité illégale, ainsi que la formation d'un espace de caractéristiques pour la classification en catégories de risque.

L'analyse d'une telle quantité de données n'est pas possible sans le recours au traitement automatique. Rosfinmonitoring a développé et a mis en œuvre avec succès plusieurs techniques d'intelligence artificielle, y compris une composante qui permet le développement, la formation et l'application de modèles mathématiques pour analyser le comportement des acteurs économiques.

Cette composante comprend un modèle de classification capable d'apprendre qui peut être utilisé dans la pratique, par exemple pour

identifier, parmi des millions d'entités commerciales, des entités dont les fondateurs et la direction sont fictifs, ou des personnes physiques fictives qui sont impliquées dans le blanchiment d'argent, ainsi que d'autres indications d'activités suspectes ou illégales.

En ce qui concerne le traitement du langage naturel, on met en œuvre la fonction d'identification du relevé d'identité bancaire recueilli suite au traitement de messages publiés dans les réseaux sociaux et présentant des signes de collecte de fonds à des fins illégales.

Le segment russophone de l'Internet est analysé de la même manière. Le composant extrait et analyse les entités présentant un intérêt pour le Service fédéral de surveillance financière et relève leurs corrélation.

Les données obtenues enrichissent l'espace informationnel de Rosfinmonitoring, en complétant les informations déjà disponibles sur les entités.

À l'ère de l'économie numérique, les énormes quantités de données accumulées et stockées offrent des opportunités uniques de trouver des informations importantes et de jouer un rôle clé dans la prise de décision, la création de nouveaux modèles basés sur des schémas et des tendances cachées, et l'optimisation des flux de travail.

Rosfinmonitoring met en œuvre un projet de plateforme internationale pour les cellules de renseignement financier de 7 pays : la République d'Arménie, la République de Biélorussie, la République du Kazakhstan, la République kirghize, la Fédération de Russie, la République du Tadjikistan et la République d'Ouzbékistan.

La plateforme technologique créée par Rosfinmonitoring, le Centre

international d'évaluation des risques de blanchiment de capitaux et de financement du terrorisme (CIER), offre à ses partenaires des méthodes innovantes pour coordonner et renforcer la coopération internationale dans l'identification et la réduction des menaces transnationales, ce qui est primordial pour le travail dans le contexte de turbulences mondiales.

La création du CIER a été conditionnée par les risques communs pour tous les pays associés de la BC/FT et par le besoin des actions communes pour les minimiser. Ces risques comprennent, entre autres, les flux financiers transnationaux suspects, l'utilisation de sociétés écrans ou des entrepreneurs individuels, les opérations d'encaissement, le trafic transnational de stupéfiants et le transfert de capitaux vers des sites de blanchiment étrangers communs.

» « LA PLATEFORME TECHNOLOGIQUE CRÉÉE PAR ROSFINMONITORING, LE CENTRE INTERNATIONAL D'ÉVALUATION DES RISQUES DE BLANCHIMENT DE CAPITAUX ET DE FINANCEMENT DU TERRORISME (CIER), OFFRE À SES PARTENAIRES DES MÉTHODES INNOVANTES POUR COORDONNER ET RENFORCER LA COOPÉRATION INTERNATIONALE DANS L'IDENTIFICATION ET LA RÉDUCTION DES MENACES TRANSNATIONALES, CE QUI EST PRIMORDIAL POUR LE TRAVAIL DANS LE CONTEXTE DE TURBULENCES MONDIALES »

La fusion de données sur les flux financiers de tous les États membres dans le cadre d'un espace

d'information unique permet de faire une analyse complexe des transactions financières dans la CEI, ainsi que de créer les conditions d'une prévision efficace des risques potentiels afin d'appliquer des mesures préventives et des barrières communes.

Une vision uniforme des risques, un échange de données rapide et avancé permettront aux États membres du Comité des chefs de CRF des membres de la CEI (CCCRF) d'appliquer efficacement des outils de réponse pour réduire les menaces communes, en concentrant les efforts spécifiquement sur le combat contre la criminalité et le renforcement de la coopération dans le cadre de la lutte contre les activités illicites.

Un aspect important de la collaboration avec les pays dans le cadre du CIER est l'amélioration de la qualité du travail analytique de la CRF en utilisant les données à la disposition des pays partenaires. La possession d'informations à jour sur l'état et la dynamique des transactions financières transfrontalières et sur les risques de BC/FT qui y sont liés permettra d'effectuer des opérations préventives internationales thématiques avec la participation de la CRF et d'autres autorités nationales des États membres du CCCRF.

La « Zone nationale de sécurité financière » est un autre élément qui permet d'assurer la surveillance financière pour protéger les intérêts nationaux de l'État. Dans ce cas, les technologies Big Data sont un outil de support à la prise de décisions et aux outils méthodologiques, logiciels et matériels informatiques nécessaires à l'amélioration qualitative des systèmes de gestion. La « Zone nationale de sécurité financière » est un système qui combine l'ensemble d'approches méthodologiques de systématisation et d'analyse de l'information, des méthodes de traitement des données et des

solutions logicielles et matérielles pour le stockage, la recherche et la visualisation de l'information.

La « Zone nationale de sécurité financière » remplit les fonctions principales suivantes :

- Analyse des données dans de différents domaines.
- Identification des interactions et l'acquisition de nouvelles connaissances entre les différents domaines de surveillance.
- Utilisation des informations reçues pour prendre des mesures opportunes de prévention, de protection ou de barrage.

Il s'agit essentiellement d'une analyse interdisciplinaire des événements dans différents domaines de surveillance. Cette analyse permet d'identifier les points de concentration des risques et les nouveaux facteurs de risque. L'intégration d'un tel système dans les processus de planification stratégique fournit une base pour les mesures d'atténuation des risques.

Il est également important de noter que les technologies de blockchain ont changé la façon dont nous faisons des affaires et ont apporté la confiance à l'époque de l'économie numérique. La technologie Blockchain garantit la sécurité et la transparence des transactions crypto dans le monde actuel. Toutefois, si les données de source (adresses de l'expéditeur et du destinataire des crypto-monnaies, montant et durée de la transaction) sont entièrement disponibles, il n'y a généralement pas d'informations permettant d'identifier les participants.

Pour résoudre ce problème, le Service utilise actuellement dans le cadre de ses activités le service d'analyse des transactions en crypto-monnaies « Blockchain transparente », qui est basé sur le marquage des participants au marché de la crypto-monnaie ce

qui permet de surveiller et de suivre leurs activités.

Bien que « Blockchain transparente » soit un produit relativement nouveau, plus de 7 000 de policiers et des agents de cellules de renseignement financier étrangères ont déjà accès au service. Le Service a déjà eu des succès dans des enquêtes financières menées conjointement avec les forces de l'ordre notamment avec des unités chargées de la lutte contre l'utilisation de crypto-monnaies pour des activités illégales, qui se sont achevées par des affaires pénales. Actuellement, des travaux sont en cours pour assurer le bon fonctionnement et le développement rapide du service, et l'on peut dire qu'il deviendra l'un des éléments clés de l'écosystème numérique de Rosfinmonitoring.

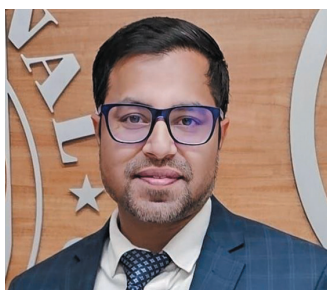
Avec le développement des technologies numériques, il existe de nouvelles exigences en matière d'éducation et de compétences nécessaires pour s'adapter et évoluer en tant qu'un spécialiste dans ce monde qui change rapidement. La culture numérique devient une partie intégrante de l'éducation. Cela prévoit d'être capable de mieux utiliser les technologies numériques, de traiter des informations, de travailler avec des données et d'utiliser des outils numériques pour résoudre des problèmes. Les programmes d'enseignement doivent être plus flexibles et adaptatifs pour garantir la prise de compétences et de connaissances appropriées. Les programmes et les méthodes d'enseignement doivent être mis à jour pour refléter les dernières tendances et exigences de l'économie numérique.

Dans ce contexte, le Service est plus que jamais intéressé par des employés possédant de haut niveau de compétences en apprentissage automatique, en Data Science, en programmation Python.



DÉVELOPPEMENT DE LA TECHNOLOGIE FINANCIÈRE EN INDE : LA POLITIQUE VISANT À STIMULER L'INNOVATION, ASSURER LA SÉCURITÉ FINANCIÈRE ET À LUTTER CONTRE LA CYBERCRIMINALITÉ

Le secteur des services bancaires numérique et mobiles en Inde a augmenté rapidement ces dernières années, ce qui est assuré par les initiatives gouvernementales visant à faciliter l'accès aux services financiers, ainsi que par le développement de l'Internet et la large distribution de smartphones à un prix abordable



➤ **M. KECHAV ANANDE**
Directeur adjoint
CRF DE L'INDE



➤ **MME M. CHANMOUGA PRIYA,**
Codirecteur
CRF DE L'INDE

L'afflux annuel de techniciens et d'experts financiers — des diplômés des universités et des collèges prestigieux de l'Inde, avec la politique gouvernementale visant à favoriser les startups et la croissance durable du PIB du pays, créent un écosystème solide qui rend possible le développement rapide des startups de la technologie financière.

La mise en œuvre de l'Interface de Paiement Unifiée (Unified Payments Interface — UPI) (service mobile de paiement instantanés) a apporté une augmentation significative. Grâce à ce service, entre janvier 2019 et janvier 2024, le nombre de transactions est passé de 672 millions jusqu'à la quantité incroyable de 12 203 millions avec le montant des transactions partant de Rs 109 932 crore (environ

15,5 milliards de dollars des États-Unis) à Rs 1 841 084 crore (environ 221,5 milliards de dollars des États-Unis)¹.

Malgré la promotion des services financiers parmi la population, le développement de la technologie financière a également créé de nouveaux risques pour la stabilité financière. En particulier, il faut

¹ <https://www.npci.org.in/what-we-do/upi/product-statistics>.

noter une forte probabilité de cybercriminalité financière. Les régulateurs et les forces de l'ordre, les services de renseignement et les représentants de l'industrie de la technologie financière sont conscients des risques auxquels nous sommes exposés. Aujourd'hui, nous travaillons ensemble pour faire face à ces risques. De plus, des mesures appropriées sont prises pour les éliminer et les partager avec le public.

ANONYMAT, ACCESSIBILITÉ DU WEB ET CROISSANCE DE LA CYBERCRIMINALITÉ

La croissance de la cybercriminalité est due à l'anonymat offert par le développement technologique et le réseau Internet. Même avec des compétences techniques minimales, une personne peut gagner de l'argent illégalement sans sortir de chez soi. Malgré des mesures de cybersécurité efficaces, il reste de certaines vulnérabilités dans les systèmes, et les malfaiteurs en profitent. Les cyberattaques qui s'appuient sur ces défaillances, et la surveillance cachée permettent de détecter ces tactiques d'intrusion. En raison de son accessibilité en réseau, le cyberspace permet d'agir à l'échelle mondiale presque sans obstacles.

RISQUE POUR LA STABILITÉ FINANCIÈRE

En novembre 2022, une évaluation nationale des risques en Inde a révélé que la cyberfraude et les défauts du système de sécurité présentent des risques importants pour la stabilité financière. C'est notamment le cas des opérations bancaires, des prêts, des paiements, des marchés boursiers et monétaires. La cybercriminalité non seulement affaiblit la crédibilité des banques,

mais crée également un certain nombre de risques : défaillances, contraintes de ressources, pertes financières, problèmes de liquidité. L'augmentation récente de la cyberfraude constitue une menace grave pour le secteur financier en termes de vulnérabilité à la LBC.

TENDANCES DE LA CYBERCRIMINALITÉ : L'AUGMENTATION DE NOMBRE DE FRAUDE FINANCIÈRE

Selon le rapport I4C² pour le deuxième trimestre de 2022 publié dans la revue Cyber Pravaha, le nombre de cybercrimes enregistrés sur le Portail national d'enregistrement des cybercrimes de l'Inde (NCRP) a atteint 237 658 contre 97 179 pour la même période de l'année précédente. La catégorie dominante était la fraude financière sur Internet — 67,9% de tous les cybercrimes enregistrés. Parmi les plateformes de paiement, c'est la fraude liée à l'UPI qui a augmenté le plus fortement, passant de 18 864 à 84 145 au deuxième trimestre par rapport à l'année précédente. En outre, les piratages des cartes de débit et de crédit ont considérablement augmenté au cours de la même période, passant de 8 628 à 26 793, ainsi que les plaintes pour une fraude bancaire sur Internet, qui sont passées de 5 104 à 19 267.

ANALYSE STRATÉGIQUE DES INSIGHTS

Le groupe d'analyse stratégique de la Cellule de renseignement financier (CRF) de l'Inde a mené une analyse approfondie des déclarations de transactions suspectes (DTS) liées à la cybercriminalité entre avril 2018 et décembre 2022. Le nombre de ces déclarations a été multiplié par 12.

Les principaux types de cybercrimes sont le piratage d'une carte de crédit, l'hameçonnage, les arnaques liées à l'offre d'emploi, le vol de données personnelles et les fausses applications de crédit/de jeux vidéo ou de pari.

Une nouvelle méthodologie basée sur l'évaluation des risques a été mise au point pour identifier et surveiller les personnes physiques et morales impliquées dans les cybercrimes. Cette méthode tient compte de la diversité des entités qui signalent des transactions suspectes, de la fréquence de ces déclarations et de l'ensemble des infractions principales.

En outre, des mesures préventives et opérationnelles ont été prises pour identifier et traiter les nids de la cybercriminalité sur la base d'analyse spatiale.

Des plans d'action ont été élaborés pour les groupes vulnérables au risque élevé de cybercrimes suite aux résultats de l'analyse stratégique basée sur l'évaluation des risques. Cela comprend l'analyse opérationnelle de ces groupes, la formation et le dialogue continu avec les entités déclarantes pour comprendre et éliminer les nouveaux schémas de cybercrimes et pour améliorer les stratégies de lutte contre le blanchiment d'argent face à l'augmentation du nombre de cybercrimes.

MESURES PRISES POUR ÉLIMINER LES RISQUES

La lutte contre la cyberfraude et le blanchiment de capitaux est facilitée par la surveillance des schémas frauduleux par la CRF de l'Inde en

² Centre indien de coordination contre la cybercriminalité (I4C), fondé par le Ministère de l'Intérieur de l'Inde en tant que Centre de coordination contre la cybercriminalité.

collaboration avec les forces de l'ordre et les organisations financières. Un groupe de travail spécial a élaboré et mis en œuvre des « signaux d'alerte », signes typiques de la cyberfraude. En même temps, l'accent a été mis sur les transactions et les schémas frauduleux identifiés dans plusieurs applications frauduleuses, y compris celles liées au crédit, aux paris, aux jeux de hasard, à l'investissement, au recrutement et aux rencontres. Les mesures renforcées comprennent désormais la surveillance des risques liés aux applications, la modification des procédures de la vérification de la fiabilité, de la vérification des adresses IP et des données de géolocalisation pour

lutter plus efficacement contre ces infractions.

En collaboration avec des entités déclarantes, la CRF de l'Inde contrôle régulièrement les applications, les sites web et les plateformes de réseaux sociaux connus pour mettre en danger des utilisateurs par le biais de divers modèles de cybercrimes. Les renseignements recueillis grâce à ces mesures sont diffusés aux entités déclarantes, aux autres services de renseignement et aux forces de l'ordre pour qu'ils prennent de nouvelles mesures. De plus, l'analyse des stratégies actuelles de lutte contre la cybercriminalité permet de sensibiliser le public et

d'aider les entités déclarantes à identifier et à combattre ces schémas illicites à l'aide de leurs systèmes de lutte contre le blanchiment de capitaux.

La banque RBI a pris une série de mesures d'atténuation des risques et publié des recommandations pour des banques comment lutter contre la fraude et la cybercriminalité. Des recommandations spéciales détaillent également les méthodes utilisées par les fraudeurs, notamment l'attaque sur de comptes bancaires et de portefeuilles d'instruments prépayés (Prepaid Instrument — PPI). Les banques doivent résoudre rapidement ces problèmes en analysant les modèles de fraude et en élaborant des stratégies pour remédier aux vulnérabilités découvertes.

La banque RBI a également publié des instructions pour des banques concernant la fraude et la cybercriminalité liée à l'investissement, aux offres d'emploi à temps partiel et aux pyramides financières. La RBI insiste sur la nécessité :

- a) de mettre en place un système fiable pour identifier et surveiller les comptes de mules bancaires présumés ;
- b) d'améliorer les procédures de vérification de la fiabilité des clients, les mesures de lutte contre le blanchiment de capitaux, y compris l'évaluation juridique complète, la vérification

EN COLLABORATION AVEC LE RÉGULATEUR, LA BANQUE DE RÉSERVE DE L'INDE (RESERVE BANK OF INDIA — RBI) ET D'AUTRES BANQUES, LA CRF DE L'INDE A FORMÉ UN GROUPE DE TRAVAIL POUR LUTTER CONTRE LES COMPTES DE MULES BANCAIRES DES CYBERCRIMINELS. DES RECOMMANDATIONS SUIVANTES ONT ÉTÉ REDIGÉES :

1. Standardiser l'identification et la prévention des comptes de mules bancaires par le biais d'évaluations des risques, de procédures de vérification de la fiabilité et de mesures technologiques.
2. Encourager l'échange d'informations entre les institutions financières afin d'empêcher le mouvement de fonds frauduleux.
3. Introduire la biométrie du comportement pour mieux détecter les infractions.
4. Attribuer un indice de risque aux comptes.
5. Créer un système de suivi des réseaux des comptes de cybercriminels.



de l'identité, le profilage des risques, la surveillance en temps réel et le traitement des comptes qui seraient utilisés à des fins illicites ;

- c) d'assurer le contrôle et la surveillance efficaces des transactions numériques, y compris dans le cadre de l'UPI, et de signaler les activités suspectes auprès de la CFR de l'Inde, même si les opérations sont gérées par des prestataires de services tiers.

INITIATIVES INSTITUTIONNELLES DE LUTTE CONTRE LA CYBERCRIMINALITÉ

En 2019, le ministère indien de l'Intérieur a créé le Centre indien de coordination contre la cybercriminalité (I4C). Le portail national d'enregistrement des cybercrimes permet de signaler 24 heures sur 24 les infractions, en particulier celles commises à l'encontre des femmes et des enfants. Le système de signalement et de gestion des cybercrimes (Citizen Financial Cyber Fraud Reporting and Management System) permet d'agir rapidement contre les cyberfraudeurs au numéro vert « 1930 ».

Le portail CyTrain offre aux forces de l'ordre une formation en ligne sur les enquêtes et les poursuites de cybercrimes. En même temps les Groupes conjoint de coordination de la lutte contre les cybercrimes renforcent la coopération interinstitutions.

Le Laboratoire national de cybercriminalité fournit des moyens d'expertise légale innovant pour mener des enquêtes sur ce type d'infractions.

Le groupe de réponse aux incidents informatiques (CERT-In) traite les incidents de sécurité informatique et favorise la mise en œuvre des meilleures pratiques. L'initiative « La cybersécurité de l'Inde » (Cyber Surakshit Bharat) est liée à la formation des informaticiens du Gouvernement en matière de cybermenaces et le programme CyberDost sensibilise le public à la cybersécurité.

Ainsi, la CFR de l'Inde, en collaboration avec les régulateurs et d'autres institutions du Gouvernement indien impliqués dans la lutte contre la cybercriminalité, fait tous ses efforts pour prévenir la cyberfraude et réduire les pertes financières causées par cette activité criminelle. Les efforts coordonnés de la CFR

de l'Inde, des CFR étrangères et des organisations sous contrôle pour prévenir le mouvement de fonds illicites sur les comptes bancaires des cybercriminels ont permis d'éviter des pertes financières à un grand nombre de citoyens et, par conséquent, de protéger l'écosystème de services financiers du pays. Grâce aux initiatives prises par le Gouvernement indien pour lutter contre la cybercriminalité, l'Inde est en bonne voie pour éliminer bientôt cette menace.

➤ **« LES EFFORTS COORDONNÉS DE LA CFR DE L'INDE, DES CFR ÉTRANGÈRES ET DES ORGANISATIONS SOUS CONTRÔLE POUR PRÉVENIR LE MOUVEMENT DE FONDS ILLICITES SUR LES COMPTES BANCAIRES DES CYBERCRIMINELS ONT PERMIS D'ÉVITER DES PERTES FINANCIÈRES À UN GRAND NOMBRE DE CITOYENS ET, PAR CONSÉQUENT, DE PROTÉGER L'ÉCOSYSTÈME DE SERVICES FINANCIERS DU PAYS »**

YOURI KOROTKI :

« LA SURVEILLANCE FINANCIÈRE EST UNE SORTE DE TOMOGRAPHIE FINANCIÈRE »



Youri Korotki parle de l'évolution des systèmes d'information de Rosfinmonitoring, le système informatique idéal du futur et la conformité dans le secteur de crypto-monnaie

Youri Korotki est Docteur en droit, juriste émérite de la Fédération de Russie, expert international dans le domaine de la lutte contre le blanchiment de capitaux et le financement du terrorisme



Ayant rejoint le Comité de surveillance financière un an après sa fondation, Youri Fedorovitch a travaillé dans le domaine du renseignement financier pendant 22 ans. Sous sa direction l'arsenal analytique a été amélioré, de nouveaux outils d'analyse ont été développés et introduits, ainsi qu'une méthodologie pour organiser le travail de la gestion des risques BC/FT.

Dans un entretien exclusif avec « Sécurité financière », Youri Korotki a expliqué comment le système informatique du renseignement financier russe s'est développé, quelles méthodes d'analyse des personnes à haut risque sont les

plus efficaces et pourquoi il est si important de réglementer la circulation des crypto-monnaies.

Youri Fedorovitch, vous avez consacré plus de 20 ans à Rosfinmonitoring. Vous avez été à l'origine des systèmes d'information du Service. Où tout cela a-t-il commencé ?

Tout système d'information (SI) est une combinaison de trois éléments : « information » + « technique » + « cerveau ». Dans le langage des technologies de l'information, il s'agit d'une ressource d'information, d'un système logiciel et matériel et d'une analyse. Lorsque j'ai rejoint le Service en novembre 2001 (à l'époque, il ne s'agissait pas du Service,

mais du Comité de surveillance financière), les parties « information » et « technique », c'est-à-dire le système de collecte, de stockage et de traitement de l'information, étaient déjà constituées. Franchement, ce n'est pas mon mérite. Je ne peux m'empêcher de citer les noms de ces merveilleux « pionniers » : Alexandre Yegorkine, Youri Grebenchchikov, Valeri Makéchine et bien d'autres.

Quant à la troisième composante analytique, on y a effectivement contribué. Et tout a commencé avec le système de comptabilité spéciale. À cette époque, il s'appelait « BCS » – le bureau de comptabilité spécial – et il réglait en détail les motifs, les fondements, les procédures d'établissement, les procédures d'enquêtes financières et leur mise en œuvre. C'est-à-dire que les algorithmes pour l'ensemble du processus de travail analytique ont été définis. Cette composante est toujours actuelle et, dans son essence, n'a guère changé depuis 20 ans. Cependant, elle a changé de nom pour devenir la « CAEF », composante d'appui aux enquêtes financières.

Nous savons que vous êtes l'auteur d'une méthodologie pour l'élaboration d'un flux de travail pour la gestion des risques BC/FT. L'une de ses idées clés est d'évaluer les risques dans le contexte. Quel est l'avantage de cette approche ?

Je dirai même plus. À mon avis, ce n'est pas seulement un avantage, c'est la seule approche correcte, car ce n'est pas l'opération elle-même qui est suspecte, mais les circonstances dans lesquelles elle a été effectuée. Par conséquent, le caractère suspect d'une transaction ne peut être évalué qu'en fonction du contexte dans lequel elle est effectuée. À mon avis, c'est évident. Par exemple, pour évaluer le caractère suspect des transactions dans le secteur public, il faut étudier les détails du marché public, le mécanisme de tarification, les particularités des procédures de sélection via l'appel



» « LE SYSTÈME INFORMATIQUE DU FUTUR RESSEMBLERA À LA TECHNOLOGIE DU CONTRÔLE AUTOMATIQUE DE LA SITUATION OPÉRATIONNELLE À FOND À L'AIDE DE MILLIERS D'INDICATEURS ET DE DONNÉES MASSIVES »

d'offre, la légitimité du choix du fournisseur, l'éventuelle affiliation du fournisseur de services avec le client et bien d'autres aspects qui représentent le contexte des transactions impliquant l'utilisation de fonds budgétaires.

La cellule du renseignement financier est une agence qui a besoin des technologies modernes d'information financière en raison de la grande quantité de données qui sont analysées chaque jour. Quelles propriétés doit avoir un système pour pouvoir s'adapter rapidement aux défis et aux menaces ? Une adaptation rapide du système, est-elle possible ?

Oui, la capacité à s'adapter rapidement aux changements de l'environnement et à répondre rapidement aux défis et aux menaces en constante évolution est sans aucun doute une exigence très importante pour un système. Mais cela ne suffit pas. Un tel système est condamné à

un « rattrapage » constant et à des défis « post factum ». Le système doit fonctionner d'une manière proactive. Comment y arriver ? Revenons à votre question précédente, il faut tenir compte du contexte. Nous ne savons pas exactement ce que le criminel va faire demain ni qu'il est en réalité. Mais nous savons où et comment il est susceptible d'agir. Je ne révélerai pas tous les secrets et les indicateurs de risque qui nous permettent d'identifier les domaines de surveillance renforcée, où le système est orienté à l'avance vers des signes et des faits possibles avant même qu'ils n'apparaissent et est prêt à y réagir. Attendre l'ennemi dans une embuscade, c'est le principe de l'action préventive. Mais cela nécessite une analyse prédictive.

Qu'est-ce que c'est, le système informatique idéal du futur pour renforcer le système anti-blanchiment ?

Suggérez-vous que nous rêvions ? J'ai depuis longtemps remarqué de nombreuses similitudes entre l'objectif d'un système de surveillance financière et la tomographie médicale. En effet, leurs tâches sont identiques : diagnostiquer une maladie à temps ou identifier les symptômes d'une maladie. La surveillance financière est une sorte de tomographie financière. Le système informatique du futur ressemblera à la technologie du contrôle automatique de la situation opérationnelle à fond à l'aide de milliers d'indicateurs et de données massives. Le résultat, comme en médecine, est l'évaluation de la santé, le diagnostic des maladies et l'élaboration d'un traitement. Et tout cela en utilisant l'intelligence artificielle. Que pensez-vous de cette image de l'avenir ?

Cela semble intéressant et prometteur. Quels sont, selon vous, les outils les plus utiles pour évaluer les menaces extérieures et les vulnérabilités intérieures d'un pays ?

En bref, aucun outil individuel n'est capable de le faire. Vous avez besoin d'un arsenal d'outils et d'un système de sélection automatique des outils adaptés a) au type de menace/vulnérabilité identifiée et b) aux spécificités du domaine dans lequel la menace/vulnérabilité se produit.

Quelles sont les tendances actuelles en matière de développement de systèmes informatiques à des fins de surveillance ?

On parle beaucoup de numérisation maintenant. Lors du cours sur le Leadership de transformation numérique, l'un des professeurs a déclaré qu'il était possible de numériser une poubelle. Mais ce que nous obtiendrons, ce n'est pas une numérisation, mais une poubelle numérique. Et c'est vrai. La transformation doit d'abord avoir lieu dans la tête de ceux dont le travail doit être numérisé. Il y a une telle

notion de « maturité numérique » que le système et ses acteurs doivent atteindre. Ce n'est pas possible d'éviter ce processus. Mais il peut et doit être accéléré. À mon avis, nous sommes dans une phase de « maturation numérique ». Qu'est-ce que c'est ? Dans les trois grandes tendances qui sont indiquées dans notre Concept, et il n'y a rien de nouveau ici :

- la compréhension et la représentation formalisée de la structure du domaine de la LCB/FT (ontologie) ;
- une approche processus, c'est-à-dire une description étape par étape du processus d'obtention des résultats finaux et des objectifs d'efficacité ;
- passer de la technologie de gestion des données à l'extraction et à la gestion des connaissances.

De la méthode de la « pupille dilatée » à l'automatisation : à votre avis, quelles sont, les méthodes les plus modernes d'analyse des opérations à risque qui sont efficaces ?

Nous nous souvenons avec ironie et sourire de la méthode de la « pupille dilatée », par laquelle nous avons commencé à analyser le flux de messages entrant. Mais en fait, le principe lui-même n'a pas changé. Tant à l'époque, il y a 20 ans, qu'aujourd'hui, ils sont basés sur ce que nous appelons des indicateurs de risque. Simplement avant, c'était la pupille de l'analyste qui réagissait, et aujourd'hui, les technologies de l'information permettent non seulement d'éliminer un signal de risque, mais aussi de mesurer le scoring, d'attribuer des zones en fonction des niveaux de risque (ce que l'on appelle le « feu de circulation »), de créer des cartes de stress de l'environnement opérationnel avec l'attribution de facteurs qui forment les « zones rouges ». La « matrice des risques

» que nous avons développée n'est pas encore totalement mise en pratique de l'analyse situationnelle et de l'évaluation des risques nationaux, mais je suis convaincu qu'il s'agit de l'avenir, et c'est là un vaste champ d'application de l'intelligence artificielle.

» « LA « MATRICE DES RISQUES » QUE NOUS AVONS DÉVELOPPÉE N'EST PAS ENCORE TOTALEMMENT MISE EN PRATIQUE DE L'ANALYSE SITUATIONNELLE ET DE L'ÉVALUATION DES RISQUES NATIONAUX, MAIS JE SUIS CONVAINCU QU'IL S'AGIT DE L'AVENIR, ET C'EST LÀ UN VASTE CHAMP D'APPLICATION DE L'INTELLIGENCE ARTIFICIELLE »

Rosfinmonitoring continue sa coopération avec les alliés et renforce sa réciprocité avec d'autres pays. En même temps, les systèmes informatiques sont différents. Quels sont les principaux mécanismes permettant de coopérer, y compris avec de nouveaux produits techniques dans le contexte des spécificités nationales ? Les technologies de l'information peuvent-elles servir d'outil pour approfondir la coopération ?

La séquence est la suivante : d'abord, les algorithmes de travail commun sont élaborés, en même temps que le cadre réglementaire est préparé, et ensuite les projets informatiques communs sont lancés. Dans ce cas, il est donc primordial d'avoir la volonté et les recherches conjointes. Si cette base est constituée, les



experts en IT n'échoueront pas. Les problèmes d'adaptation et d'intégration de différents systèmes sont techniquement difficiles, mais la solution existe. L'essentiel est la formation d'un espace opérationnel commun et d'approches communes pour son exploitation.

Que pensez-vous de l'évolution de la conformité compte tenu de la nécessité de réglementer les crypto-actifs ?

Le terme « compliance » signifie « conformité aux règles ». Par conséquent, le développement du système de conformité dans le domaine du commerce des crypto-actifs dépend directement de la rapidité avec laquelle nous parviendrons à un système complet de régulation du marché des crypto-monnaies. Au stade actuel, où la conformité fonctionne exclusivement dans le domaine

de la circulation de la monnaie fiduciaire, nous devons compléter le système de contrôle interne en cours par des méthodes et des outils permettant de découvrir des « liens » entre les opérations bancaires des clients et leurs transactions de crypto-monnaies. Il faut apprendre à reconnaître cette liaison via soi-disant les « mules financières », les paiements P2P et d'autres points de connexion entre deux systèmes d'exploitation différents : les devises fiduciaires et les crypto-monnaies. C'est exactement de ce problème que nous nous occupons dans le cadre du projet « Blockchain transparente » par délégation du président de la Fédération de Russie.

Quant aux perspectives de la réglementation du marché national des crypto-monnaies, je suis convaincu qu'elles ne devraient pas suivre la voie de « déplacement » des transactions de crypto-monnaie dans la circulation parallèle, mais, au contraire, celle de l'amélioration de leur transparence. Le deuxième domaine important est celui

de l'intermédiation des crypto-monnaies. Ce qu'il faut ici, c'est la « substitution aux importations » des prestataires de services en actifs virtuels étrangers (PSAV) et l'établissement d'un marché national de services de crypto-monnaie doté de son propre système de conformité de la crypto-monnaie. En outre, nous avons l'expérience « embarquement » de grands fournisseurs étrangers de technologies informatiques dans des conditions de conformité avec la législation russe, y compris la législation fiscale et la législation relative à la lutte contre le blanchiment d'argent. Cette expérience devrait également être appliquée aux PSAV non-résidents. L'activité sans entrave des bureaux d'échange de crypto-monnaies étrangers sur le territoire de la Russie, tout en restant en dehors de la juridiction russe, ou plus précisément, dans la zone des « trous de réglementation » de la législation russe, ce qui comporte des risques encore plus grands que la crypto-monnaie elle-même. L'élimination de ces « trous » est inutilement retardée.

» « QUANT AUX PERSPECTIVES DE LA RÉGLEMENTATION DU MARCHÉ NATIONAL DES CRYPTO-MONNAIES, JE SUIS CONVAINCU QU'ELLES NE DEVRAIENT PAS SUIVRE LA VOIE DE « DÉPLACEMENT » DES TRANSACTIONS DE CRYPTO-MONNAIE DANS LA CIRCULATION PARALLÈLE, MAIS, AU CONTRAIRE, CELLE DE L'AMÉLIORATION DE LEUR TRANSPARENCE »



RÉGLEMENTATION DU MARCHÉ DES TECHNOLOGIES FINANCIÈRES DANS LE CONTEXTE DE LBC/FT : L'EXPÉRIENCE DE L'OUBÉKISTAN



OTABEK RAKHMANOV,

Directeur adjoint de la Direction de la Banque Centrale de la République d'Ouzbékistan

La population totale de l'Ouzbékistan est de 36,5 millions d'habitants dont des jeunes âgés de 15 ans et plus constituent une grande partie. Cela constitue une base potentielle pour élargir la technologie financière, compte tenu de la tendance des jeunes à adopter de nouvelles solutions numériques

APERÇU DU MARCHÉ DES TECHNOLOGIES FINANCIÈRES : ENTITÉS

Le marché comprend 35 banques avec un réseau de 2 510 agences et bureaux des services bancaires. Cela garantit une large couverture du territoire national et l'accès aux services financiers pour la population.

L'Ouzbékistan compte 49 établissements de paiement, ce qui témoigne de la variété des services financiers proposés. De plus, il existe 12 systèmes de monnaie électronique et 6 systèmes de paiement, ce qui favorise la diversité et la concurrence sur le marché.

Il existe trois opérateurs de systèmes de paiement sur le marché qui assurent une infrastructure pour des virements de fonds et des transactions efficaces.

Ces données soulignent l'importance du secteur financier de l'Ouzbékistan et suggèrent que le pays dispose d'une infrastructure bien développée pour diverses transactions financières, ce qui crée des conditions favorables au développement des technologies financières.

APERÇU DU MARCHÉ DES TECHNOLOGIES FINANCIÈRES : OBJETS

Plus de 427 000 terminaux de paiement électronique (TPE) fonctionnent dans le pays, ce qui est un chiffre important qui montre une large diffusion des systèmes de paiement sans numéraire dans les commerces et les points de services.

Il y a plus de 24 000 guichets automatiques et bornes interactives. Cela veut dire que la majorité de la population dispose d'accès aux

services financiers, étant donné que ces installations sont souvent situées à la fois dans les agences bancaires et dans les lieux publics.

Il y a 42,4 millions de cartes de paiement en circulation ce qui indique l'utilisation massive de la monnaie électronique dans le pays. C'est très commode pour les consommateurs et favorise le développement des paiements sans numéraire.

6,7 millions de cartes bancaires utilisent les systèmes de paiement internationaux tels que Visa, UnionPay, Mastercard. Cela signifie que le système financier ouzbek s'est intégré dans l'économie mondiale et permet aux citoyens et au commerce d'effectuer des transactions internationales.

Ainsi, les institutions financières qui utilisent la technologie financière en Ouzbékistan proposent une large gamme et permettent de fournir des services différents au niveau national et international.

MARCHÉ DES TECHNOLOGIES FINANCIÈRES : CADRE LÉGAL

En Ouzbékistan, la régulation du marché des technologies financières repose sur un certain nombre d'actes législatifs et de règles visant à garantir la sécurité et à lutter contre les activités criminelles. L'un des documents clés est la loi n° 660-II du 26 août 2004 de la République d'Ouzbékistan « Sur la lutte contre le blanchiment de capitaux, le financement du terrorisme et de la prolifération des armes de destruction massive ». Cette loi définit les principales mesures de lutte contre la criminalité financière et définit la responsabilité en cas de crime.

Des mesures supplémentaires pour la mise en œuvre de cette loi ont été approuvées par l'Ordonnance adoptée par le Cabinet des ministres

n° 402 du 29 juin 2021, ce qui indique l'amélioration continue du cadre légal dans ce domaine. Ces mesures comprennent des dispositions et des instructions spécifiques pour lutter efficacement contre le blanchiment de capitaux d'une manière efficace, le financement du terrorisme et la prolifération des armes de destruction massive.

Les règles de contrôle interne approuvées par la Banque centrale et la Cellule de renseignement financier constituent un aspect important de la réglementation. Ces règles sont destinées aux banques, aux opérateurs de systèmes de paiement, aux opérateurs de systèmes de monnaie électronique, aux établissements de paiement et visent à renforcer les mesures de lutte contre la criminalité financière.

Des dispositions sur la procédure d'identification numérique des clients ont été établis et approuvés par la Banque centrale sous le n° 3322 du 30 septembre 2021 pour assurer la sécurité des transactions et l'identification des clients. Cela permet d'identifier les clients d'une manière efficace en ligne et de réduire le risque de fraude financière.

NOUVELLES TECHNOLOGIES FINANCIÈRES : ÉTAPES DE LA MISE EN ŒUVRE DANS LES AFFAIRES

La mise en œuvre de nouvelles technologies financières dans les affaires exige plusieurs étapes d'analyse approfondie et des précautions pour garantir des opérations sûres et efficaces.

La première étape est une étude du produit qui implique un examen détaillé de ses fonctions, des caractéristiques et des avantages potentiels pour le commerce et

les clients. Ensuite, les risques, les menaces et les vulnérabilités liés au nouveau produit sont identifiés afin de bien comprendre les conséquences négatives possibles de son utilisation.

Après cela, les risques sont analysés. L'analyse des risques consiste à évaluer la probabilité des différentes menaces et leur effet potentiel sur le commerce et les clients. Des stratégies d'atténuation des risques sont élaborées sur la base des résultats d'analyse. Elles peuvent inclure des modifications du produit, des processus d'utilisation ou des politiques de sécurité de l'entreprise.

Une étape importante consiste à informer la Banque centrale avant de lancer un nouveau produit. Cela est nécessaire pour assurer la cohérence avec les dispositions de la législation et la réglementation du marché financier. Sur notification, la Banque centrale peut procéder à sa propre analyse du produit et formuler des recommandations en vue d'améliorations ou de mesures de sécurité supplémentaires.

Finalement, après avoir reçu les recommandations et l'approbation de la Banque centrale, le nouveau produit est lancé sur le marché. Cependant, le processus ne s'arrête pas là. Au moins une fois par an, les risques des produits précédents et actuels sont reidentifiés dans le contexte de la lutte contre le blanchiment de capitaux et le financement du terrorisme. Cela permet de répondre rapidement aux changements de l'environnement et d'apporter des modifications dans les stratégies de sécurité et de gestion des risques.

TECHNOLOGIES FINANCIÈRES : SOLUTIONS D'IDENTIFICATION NUMÉRIQUE

Les technologies financières jouent un rôle clé pour garantir la sécurité et l'efficacité des transactions

financières, l'identité numérique est un élément important de ce processus. Des solutions nationales d'identité numérique ont été développées en Ouzbékistan qui permettent d'identifier uniquement les résidents du pays.

L'un des principaux mécanismes utilisés dans le domaine de l'identité numérique est Liveness Detection. Ce mécanisme protège contre les attaques par piratage d'identité. Il utilise des réseaux de neurones bien formés pour vérifier si la photo présentée appartient à un utilisateur réel.

Un autre aspect important est Face Recognition qui permet de comparer un seul visage avec toutes les photos de visage de la base de données. Cette technique permet d'identifier un visage parmi plusieurs, ce qui augmente la précision de l'identification.

Face Comparison est une autre technique importante pour vérifier la probabilité que deux photos de visage appartiennent à la même personne. Cette approche est particulièrement utile pour confirmer l'identité lorsque différentes photos ou images sont utilisées.

Diverses techniques peuvent être utilisées dans l'identification numérique, y compris des processus automatisés sans assistance humaine et des techniques avec assistance humaine. Dans les deux cas, il est important d'assurer la précision et la sécurité de l'identification afin de protéger les intérêts des clients et de respecter les exigences réglementaires.

TECHNOLOGIES FINANCIÈRES : SEUILS DE TRANSACTIONS SUSPECTES

Les règles de contrôle interne relatives à la lutte contre le blanchiment de capitaux, le financement du terrorisme et de la prolifération des armes de

destruction massive (LBC/FT) en République d'Ouzbékistan fixent un certain nombre de seuils et de critères spécifiques pour déterminer les transactions financières suspectes. Ces règles visent à garantir la sécurité des transactions financières et à empêcher leur utilisation à des fins illégales.

LE MARCHÉ DES ÉTABLISSEMENTS DE PAIEMENT

Le marché des établissements de paiement en Ouzbékistan se caractérise par une vaste gamme de mesures et d'instruments adoptés et utilisés pour minimiser les risques

de blanchiment de capitaux et de financement du terrorisme (BC/FT). Afin de garantir la sécurité et la fiabilité du système monétaire du pays, les établissements de paiement mettent en œuvre diverses techniques et procédures :

Systèmes CDD (Customer Due Diligence) et KYC (Know Your Customer) : ces systèmes permettent d'identifier les clients et de vérifier qu'ils respectent les normes et les exigences des organismes de réglementation. Ils comprennent e-KYC (système de contrôle électronique des clients) qui permet d'effectuer l'identification d'une manière plus efficace et plus rapide.

LES PRINCIPAUX SEUILS POUR LES TRANSACTIONS SUSPECTES EN VERTU DES RÈGLES DE CONTRÔLE INTERNE LBC/FT EN OUZBÉKISTAN PEUVENT INCLURE LES ASPECTS SUIVANTS :

- transfert de fonds d'une carte bancaire via une application mobile vers une ou plusieurs cartes bancaires ou portefeuilles électroniques effectué par le client en une seule fois ou à plusieurs reprises dans un délai maximum de 30 jours, pour un montant total égal ou supérieur à 500 fois le montant de la valeur de calcul de base ;
- réception par le client de fonds provenant d'une ou de plusieurs cartes bancaires ou de portefeuilles électroniques pour un montant total égal ou supérieur à 500 fois la valeur calculé de base en une seule fois ou à plusieurs reprises dans un délai maximum de 30 jours ;
- transfert de fonds via une application mobile à partir de 5 cartes bancaires (portefeuilles électroniques) ou plus vers un portefeuille électronique étranger en une seule fois ou à plusieurs reprises dans un délai maximum de 30 jours ;
- réception de fonds sur 5 cartes bancaires (portefeuilles électroniques) ou plus à partir d'un portefeuille électronique étranger en une seule fois ou à plusieurs reprises dans un délai maximum de 30 jours ;
- transfert de fonds via une application mobile d'une carte bancaire (portefeuille électronique) vers 5 cartes bancaires ou portefeuilles électroniques étrangers ou plus, en une seule fois ou à plusieurs reprises dans un délai maximum de 30 jours ;
- réception de fonds provenant de 5 cartes bancaires ou portefeuilles électroniques étrangers ou plus sur une carte bancaire (portefeuille électronique) en une seule fois ou à plusieurs reprises dans un délai maximum de 30 jours.

Politiques et procédures internes : les établissements de paiement élaborent des politiques et des procédures internes pour l'interaction de leurs employés, agents et sous-agents avec les clients. Cela comprend la définition de la manière de traiter les clients risqués (personne politiquement exposée) (PPE).

Systèmes de surveillance des transactions clients : les établissements de paiement utilisent des systèmes de surveillance spécialisés qui suivent et analysent automatiquement les transactions des clients afin d'identifier les transactions suspectes.

Systèmes de détection et de transmission des transactions suspectes : les établissements de paiement disposent de mécanismes permettant de détecter et de transmettre les transactions suspectes aux autorités compétentes de surveillance et de contrôle.

Systèmes d'analyse et de surveillance des risques : les établissements de paiement analysent, évaluent et suivent régulièrement les risques liés aux transactions en cours. Ils élaborent et appliquent des stratégies d'atténuation des risques en fonction des menaces identifiées.

Élaboration et mise à jour de la réglementation interne : les établissements de paiement mettent régulièrement à jour leurs réglementations et procédures internes compte tenu des risques identifiés et des changements législatifs. Cela leur permet de répondre d'une manière efficace aux nouvelles menaces et aux exigences réglementaires.

Toutes ces mesures et tous ces instruments contribuent à lutter d'une manière efficace contre le blanchiment de capitaux et le

financement du terrorisme dans le secteur financier de l'Ouzbékistan afin de garantir la stabilité et la sécurité du système financier du pays.

SYSTÈMES DE MONNAIE ÉLECTRONIQUE

Les systèmes de monnaie électronique jouent un rôle important dans l'infrastructure moderne des marchés financiers de l'Ouzbékistan. Conformément à la législation du pays, seules les banques peuvent agir en tant qu'émetteurs de monnaie électronique, ce qui offre un niveau supplémentaire de sécurité et de contrôle sur les transactions effectuées avec des fonds électroniques.

Toutefois, il convient de noter que parfois les clients ne sont pas vérifiés d'une manière appropriée. Si le montant d'une transaction en monnaie électronique ne dépasse pas un certain seuil (par exemple, 1 valeur calculée de base) ou si le montant de monnaie électronique dans le portefeuille du client reste insignifiant (par exemple, moins de 5 valeurs calculées de base). Ces restrictions visent à simplifier et à accélérer les transactions petites et fréquentes tout en réduisant le fardeau bureaucratique sur les clients.

Des limites ont été fixées à la fois pour les transactions individuelles et pour le volume total des transactions au cours d'une période donnée pour minimiser les risques liés aux transactions de monnaie électronique. Par exemple, on peut définir le montant maximum d'une transaction de monnaie électronique, le montant maximum de monnaie électronique qui peut se trouver dans le portefeuille d'un client, le montant maximum

des transactions de monnaie électronique pendant un mois, ainsi que le montant maximum des transactions de carte bancaire par mois. Ces limites permettent aux banques et aux organismes de réglementation de contrôler et de limiter les risques potentiels liés à l'utilisation de la monnaie électronique et d'assurer la sécurité et la stabilité du système financier.

NOUVELLES TECHNOLOGIES FINANCIÈRES : NFC, CODES QR, TAP-TO-PHONE

Ces dernières années, les nouvelles technologies financières telles que NFC, codes QR et Tap-to-phone font partie intégrante du système de paiement moderne. Ils sont devenus le mode de paiement préféré de nombreux utilisateurs, car ils permettent d'effectuer les transactions d'une manière plus rapide et plus commode.

Les paiements NFC sont l'un des plus populaires parmi les modes de paiement sans contact. Le nombre de transactions utilisant cette technologie a considérablement augmenté au cours des dernières années, ce qui indique la popularité croissante de ce mode de paiement. Par exemple, en 2021, le nombre de transactions s'est élevé à 12,2 milliards de sums, et en 2023, il a déjà atteint 31,6 milliards de sums. Malgré cela, les établissements financiers doivent respecter les normes de vérification de la clientèle, en particulier dans le cas de transactions douteuses. Si cette vérification n'est pas possible, les établissements financiers sont tenus d'en informer les autorités nationales compétentes et de refuser de coopérer avec le client.

LES PAIEMENTS PAR CODE QR SONT ÉGALEMENT DEVENUS UN MODE DE PAIEMENT EN LIGNE POPULAIRE. LE VOLUME ET LE NOMBRE DES TRANSACTIONS PAR CODE QR ONT CONSIDÉRABLEMENT AUGMENTÉ CES DERNIÈRES ANNÉES.

Par exemple, en 2023, le volume de transactions s'élevait à 315 milliards de sums, et le nombre de transactions a atteint 93,8 mille sums. Cette croissance amène une attention accrue sur la sécurité et la prévention de la fraude, en particulier pour les non-résidents, les PPE et les clients effectuant des transactions suspectes.

La technologie Tap-to-phone permet d'utiliser des appareils mobiles comme terminaux de paiement électronique, ce qui réduit les coûts et augmente la commodité pour les entrepreneurs. Toutefois, il est de plus en plus nécessaire de renforcer les mesures de vérification de la clientèle. Il s'agit notamment d'obtenir des informations sur les sources de fonds et d'examiner les objectifs, les transactions prévues ou exécutées par le client.

En général, le développement des nouvelles technologies financières offre de nouvelles possibilités aux utilisateurs, mais exige des établissements financiers qu'ils portent une attention constante aux questions de sécurité et de respect des lois.

NOUVELLES TECHNOLOGIES FINANCIÈRES : FACEPAY, ATTO ET PALMPAY

En septembre 2023, une technologie innovante de paiement sans contact a été mise en œuvre, c'était une étape importante dans la technologie financière. Cette technologie, connue sous le nom de FacePay, offre un mode de paiements commode et sûr en utilisant le système de reconnaissance faciale. Une caméra spéciale lit les caractéristiques faciales uniques de l'utilisateur et les associe automatiquement à la carte bancaire liée au système, ce qui assure la sécurité et la protection des données.

En outre, une solution appelée ATTO qui est une carte bleue sans contact dotée de la technologie NFC, a été introduite dans le transport. On peut acheter les cartes ATTO dans les distributeurs de cartes spéciaux ou dans des points de vente de titres de transport, ce qui les rend accessibles à un grand nombre d'utilisateurs. Cette technologie permet également de payer les frais de transport via une application mobile, en utilisant

à la fois le protocole NFC et les codes QR, ce qui offre la commodité et la flexibilité aux passagers.

Des banques innovantes ont également introduit de nouveaux modes de paiement utilisant la biométrie de visage et par empreinte palmaire. Par exemple, les technologies FacePay et PalmPay

➤ « LE DÉVELOPPEMENT DES NOUVELLES TECHNOLOGIES FINANCIÈRES OFFRE DE NOUVELLES POSSIBILITÉS AUX UTILISATEURS, MAIS EXIGE DES ÉTABLISSEMENTS FINANCIERS QU'ILS PORTENT UNE ATTENTION CONSTANTE AUX QUESTIONS DE SÉCURITÉ ET DE RESPECT DES LOIS »

permettent aux clients d'effectuer des paiements et des transactions dans les établissements bancaires en scannant leur visage ou leur paume, ce qui renforce la sécurité et l'identification. Ces modes de paiement sont particulièrement utiles pour les clients qui apprécient la simplicité et la commodité des transactions financières.

UTILISATION DES TECHNOLOGIES NUMÉRIQUES DANS LA SURVEILLANCE ET L'AUGMENTATION DU NIVEAU DE CONNAISSANCES DES ORGANISATIONS RESPONSABLES

Les technologies numériques et les solutions automatisées pour le traitement de grands ensembles de données deviennent un élément intégré de surveillance dans le domaine de la lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT), de la mise en œuvre d'une approche fondée sur le risque, ainsi que de l'évaluation de l'efficacité et des communications avec les entités surveillées, et de l'automatisation des processus opérationnels individuels. Les objectifs de la numérisation sont d'accroître la vitesse d'interaction avec les personnes contrôlées, de réduire la charge administrative pesant sur les entreprises et de libérer les ressources des autorités de la surveillance



> VICTORIA KAPARTCHOUK,
Conseillère de la Direction de l'organisation de la surveillance de Rosfinmonitoring (Service fédéral de surveillance financière)



> YANA BAÏRATCHNAÏA,
Spécialiste -expert principal de la Direction de l'organisation de la surveillance de Rosfinmonitoring (Service fédéral de surveillance financière)



> ALEXANDRE KOURIANOV,
Chef de la Direction de l'organisation de la surveillance de Rosfinmonitoring (Service fédéral de surveillance financière), docteur en sciences économiques

Selon certaines estimations d'experts, au cours de la dernière décennie, dans le monde entier l'intensité des changements dans les réglementations du secteur du crédit et de la finance a été multipliée par plus de cinq. Par ailleurs, les cas de responsabilisation des acteurs

du marché augmentent, et les amendes pour non-respect des exigences obligatoires sont de plus en plus fréquentes et importantes. Les solutions RegTech (*Regulatory Technology*) permettent d'optimiser le processus de respect des exigences obligatoires dans le contexte d'un nombre sans cesse croissant des

exigences réglementaires. Le développement actif de la RegTech a eu lieu en 2017-2019, une période marquée par l'augmentation du fardeau réglementaire et le développement simultané des technologies d'intelligence artificielle.

LES EXPERTS SOULIGNENT UN CERTAIN NOMBRE D'AVANTAGES DES SOLUTIONS REGTECH :

Augmentation de rendement

Les technologies sont capables de traiter d'importantes quantités de données à grande vitesse, telles que l'analyse rapide de textes juridiques bruts et l'extraction des informations nécessaires à des fins de contrôle.

Précision accrue et exhaustivité

Les processus manuels et disparates ont tendance à créer des lacunes en matière de conformité, ce qui entraîne des erreurs humaines et un risque réglementaire accru. La mise en œuvre de RegTech, ainsi que l'intégration raisonnée de ces technologies, permet de remplir les lacunes et de simplifier le processus de réglementation.

Cohérence et coordination internes

Les outils technologiques offrent une plus grande transparence dans l'ensemble de l'entreprise, en rapprochant des processus et des personnels autrefois disparates. Il en résulte un environnement d'information unifié réunissant les différentes unités de l'organisation. L'échange de données est ainsi plus rapide, ce qui permet également d'améliorer la conformité.

Gestion de qualité des risques

De nombreux outils RegTech contribuent à atténuer efficacement divers types de risques, notamment les abus de marché, les cyberattaques et la fraude, en surveillant et en signalant les activités suspectes.

collecte et d'analyse des données, notamment en automatisant les tâches de routine, en développant de nouvelles méthodes d'analyse et en organisant les informations traitées.

Bien qu'il y ait quelques variantes quant à ce qui relève de SupTech, le terme a été utilisé à l'origine pour dénoter les pratiques de surveillance des acteurs du marché des valeurs mobilières. Par exemple, l'Organisation de coopération et de développement économiques note l'efficacité des solutions SupTech pour une détection plus efficace des transactions d'initiés, des manipulations de marché et autres².

Le concept SupTech est désormais envisagé pour un plus grand nombre d'autorités de surveillance, notamment celles qui contrôlent la concurrence, le respect des exigences en matière de lutte contre la corruption, et d'autres. Les experts notent que SupTech, en améliorant les capacités de surveillance, d'analyse et d'application des lois des autorités compétentes, assure un effet positif sur la stabilité financière, l'intégrité du marché et le bien-être des consommateurs³. Les instruments SupTech élargissent également les possibilités des autorités de surveillance pour améliorer leurs capacités de collecte et de gestion des données, ce qui peut à son tour améliorer la qualité des données, ce qui est une condition préalable à une analyse avancée de ces données.

La pratique de l'application de SupTech permet de souligner les principaux avantages de leur mise en œuvre par les autorités de surveillance :

Les solutions SupTech (*Supervisory Technology*) contribuent également à optimiser le respect des exigences obligatoires.

SupTech fait référence à l'utilisation d'outils numériques, y compris le matériel informatique et les logiciels, par les organismes de réglementation et de surveillance pour exercer leurs fonctions¹.

La demande pour ce type de technologies capables de collecter, de stocker, d'analyser et d'afficher différents types d'informations est due à l'intensité et au volume croissants de la création de données structurées et non structurées. Par exemple, en plus des modèles de rapports traditionnels des

entités déclarantes, les autorités compétentes utilisent activement des informations de sources ouvertes (par exemple, les publications sur les réseaux sociaux) pour élargir leurs connaissances.

Comme les autorités de régulation, de surveillance et les forces de l'ordre s'appuient sur des données, des procédures internes et des outils de travail, ainsi que sur des ressources humaines et autres, ils sont tous confrontés à des défis communs, bien qu'à des degrés divers, liés à la mauvaise qualité des données et à des procédures manuelles à forte demande de main d'œuvre. Les solutions SupTech peuvent aider les autorités compétentes à résoudre ces problèmes en améliorant leurs capacités, leur efficacité et leur rendement en matière de

¹ Going Digital : Shaping Policies, Improving Lives / OECD Publishing. URL : Mode of access : <https://doi.org/10.1787/9789264312012-en>.

² Using digital technologies to improve the design and enforcement of public policies // OECD. URL : <https://dx.doi.org/10.1787/99b9ba70-en>.

³ The Use of Supervisory and Regulatory Technology by Authorities and Regulated Institutions // Financial Stability Board. URL : <https://www.fsb.org/wp-content/uploads/P091020.pdf>.

Amélioration de la capacité de détection des infractions

Les données disponibles indiquent que les autorités de surveillance, y compris celles qui surveillent le marché des valeurs mobilières, le respect des exigences de contrôle de la concurrence et les organismes chargés de l'application de la loi impliqués dans la lutte contre la corruption, utilisent de plus en plus les instruments SupTech pour mieux détecter les infractions suivantes :

- blanchiment de capitaux et financement du terrorisme, transactions d'initié et d'autres types d'actes illicites (tels que les ventes illicites et la fraude) ;
- pratiques anticoncurrentielles ;
- faits de corruption à l'étranger.

Pour ce faire, les applications SupTech, y compris celles basées sur l'utilisation de l'intelligence artificielle, sont particulièrement pertinentes, car la surveillance repose sur l'analyse de grandes quantités de données détaillées, urgentes et non structurées provenant de sources disparates. Par ailleurs, l'identification et la lutte contre les technologies numériques facilitant l'émergence de nouvelles formes de BC/FT, de mauvaises pratiques sur les marchés financiers, de fraudes et de pratiques anticoncurrentielles, nécessitent de nouveaux outils.

Les outils d'intelligence artificielle sont utilisés par les cellules de renseignement financier pour analyser les flux d'informations entrant c'est-à-dire séparer, combiner et définir les priorités des données indiquées dans les déclarations de transactions suspectes ou d'activité du client.

Les organismes de contrôle mettent en œuvre des outils d'intelligence

artificielle pour détecter les infractions dans les marchés publics et vérifier les rapports de corruption. Au Brésil, par exemple, la technologie de l'intelligence artificielle est utilisée pour examiner les rapports de corruption reçus et décider quels cas méritent une enquête plus approfondie, ainsi que pour analyser les signaux qui identifient les procédures illégales de marchés publics avant que les contrats ne soient signés.

Amélioration de l'efficacité des pratiques d'application de la loi

Les outils d'intelligence artificielle peuvent considérablement améliorer l'efficacité des pratiques d'application de la loi, car les enquêtes et les poursuites ont tendance à utiliser beaucoup de temps et de ressources. Dans ce contexte, ces outils peuvent être efficaces pour analyser de grands ensembles de données, s'assurer que les documents présentés répondent aux exigences de format et de structure ainsi que pour analyser les preuves à l'aide de techniques d'apprentissage machine telles que le traitement automatique des langues (*Natural Language Processing*). En général, lesdits outils sont particulièrement bien adaptés à la standardisation des procédures et aux tâches périodiques impliquant de grandes quantités de données.

Amélioration de la collecte de données

Comme la déclaration obligatoire devient plus complexe, les organismes de contrôle ont du mal à recueillir des rapports tardifs et de mauvaise qualité, ce qui peut avoir un impact négatif sur leur capacité de suivi. Dans le même temps, les organisations responsables supportent des coûts importants pour rendre compte aux autorités de surveillance.

Afin d'améliorer la collecte des données, les organismes de contrôle ont commencé ces dernières années à introduire des technologies dites « pull » qui permettent aux autorités d'obtenir des données de l'entité réglementée en temps requis. Les API facilitent aux organisations responsables la présentation de ces données, ce qui réduit les frais concernés et permet une meilleure communication entre les parties⁴. Les organes de surveillance étudient les moyens de convertir les instructions de préparation de rapports au format machine afin d'automatiser les rapports réglementaires et de rendre le respect des exigences plus simple.

Amélioration de la gestion des données

Les trois tâches principales de la gestion des données sont la validation, la consolidation et la visualisation, chacune d'entre elles étant liée à des points cibles spécifiques dans le cycle de gestion des données. La validation consiste à vérifier l'intégrité, l'exactitude et la cohérence des données conformément aux règles de préparation de rapports, tandis que la consolidation concerne l'agrégation de données provenant de sources multiples et sous différents formats, et la visualisation consiste à présenter les informations de manière évidente⁵.

Les exemples de mise en œuvre de SupTech et de RegTech dans les activités des organes de surveillance de pays étrangers, y compris les États membres de l'EAG (Groupe eurasiatique pour LBC/FT), sont intéressants.

⁴ The Use of Supervisory and Regulatory Technology by Authorities and Regulated Institutions // Financial Stability Board. URL : <https://www.fsb.org/wp-content/uploads/P091020.pdf>.

⁵ The Suptech Generations // di Castri, S. et al. URL : <https://www.bis.org/fsi/publ/insights19.htm>.

En général, en ce qui concerne les activités de surveillance de la LBC/FT, les domaines suivants peuvent être distingués pour l'utilisation de solutions numériques :

- surveillance à distance des activités des personnes contrôlées en vue de l'utilisation ultérieure des informations obtenues dans les modèles d'évaluation des risques ;
- assistance à la vérification et à l'évaluation de qualité des clients et des risques qu'ils présentent ;
- fourniture du feedback, communication automatisée aux personnes contrôlées à propos de l'évaluation des risques, des informations sur les signes observés de violation des exigences obligatoires ;
- organisation de mesures préventives (mise en place de matériel de formation, y compris des cours vidéo, des questionnaires, la création de sections FAQ), etc.



Ainsi, l'Agence de la surveillance financière de la République du Kazakhstan, en utilisant la possibilité du service en ligne « Espace personnel » sur son portail, vérifie quotidiennement le travail des entités de la surveillance financière primaire, et a la possibilité de répondre rapidement aux signes de violations de la LBC/FT. L'espace personnel est utilisé pour envoyer des messages à la CRF, ainsi que pour communiquer des listes de sanctions financières ciblées pour le FT, la formation des principales entités de surveillance financière (législation anti-blanchiment, recommandations, mémos, rapports d'analyse,

description des typologies, etc.), la publication de diverses données relatives à la LBC/FT, ainsi que le feedback. L'introduction de l'Espace personnel a permis d'optimiser l'interaction avec le secteur privé, notamment en réduisant le traitement des documents.



La CNBV (Comisión Nacional Bancaria y de Valores) du Mexique, qui est responsable de la supervision de la lutte contre BC/FT, met en œuvre un projet qui inclut l'informatique en nuage pour traiter d'importants volumes de données relatives à la conformité à LBC/FT, augmentant ainsi la capacité et la flexibilité du stockage, la mobilité et la puissance du calcul. Cette plateforme permet également de développer des analyses prospectives de base et avancées afin d'améliorer l'efficacité de la surveillance et de mieux identifier les modèles de comportement inhabituels.



Singapour a mis en place des solutions informatiques pour classer les organisations par niveau de risque. L'approche de l'évaluation du risque inhérent aux banques implique généralement la collecte régulière de certaines données agrégées auprès de chaque banque afin d'estimer le niveau approprié de risque de BC/FT. Il s'agit souvent d'un processus laborieux et long, qui implique la comparaison de données entre banques comparables et peut exiger un nombre important d'évaluations qualitatives.

L'organe de surveillance de Singapour, en coordination avec des analystes de données, a dressé une liste complète des indicateurs de risque de BC/FT, a élaboré un formulaire pour collecter les données nécessaires dans un format de machine et mis au point une méthodologie d'évaluation

des risques pour son application méthodique.

Aujourd'hui, une évaluation intégrée du risque de BC/FT de chaque banque, accompagnée d'un rapport sur les principaux facteurs qui l'ont influencée, peut être rapidement créée une fois que les données sont disponibles ce qui permet aux organes de surveillance de mieux identifier les établissements financiers à haut risque. En outre, si des changements importants et inattendus dans le profil à risque de certaines banques sont identifiés à titre permanent, des mesures de surveillance peuvent être prises rapidement à leur égard.

À Singapour, les techniques d'analyse de réseau sont activement utilisées dans la surveillance de la BC/FT. Les déclarations d'activité suspecte (DAS) constituent l'une des sources de données. En utilisant des techniques d'analyse de réseau, les organes de surveillance ont développé un outil analytique pour identifier les réseaux de personnes morales et physiques qui sont connectés par le biais de différentes DAS déposées à des moments différents par différentes entités responsables. Ces données sont comparées aux informations et au profil de l'entreprise figurant dans ce que l'on appelle le Registre du commerce et des sociétés (par exemple, des informations sur les activités commerciales, les dirigeants et les bénéficiaires effectifs). En effectuant des analyses de réseau de cet ensemble de données multidimensionnelles, les organes de surveillance peuvent identifier les zones à haut risque et les établissements financiers sur lesquels exercer des activités de surveillance ciblées.

La technologie peut également modifier la manière dont sont effectués les contrôles sur place. Par exemple, les organes de surveillance utilisent des outils analytiques

automatisés pour examiner l'ensemble des transactions effectuées par l'organisation auditée au cours des deux ou trois années précédentes. Grâce à cette technologie, les inspecteurs n'ont plus besoin d'examiner manuellement les données des transactions pour identifier les anomalies. En fin de compte, cela permet à l'organe de contrôle de se concentrer sur les zones à haut risque lors des audits et facilite un dialogue plus significatif avec l'entité contrôlée et ses dirigeants sur la gestion des risques et les contrôles internes, avec des débats à propos d'exemples concrets.



En Tunisie, les organes de surveillance utilisent la technologie Blockchain pour évaluer les risques des mouvements transfrontières d'argent liquide et pour mener une surveillance ciblée des organisations. L'évaluation nationale des risques de la Tunisie en 2017 a classé le transport international d'argent liquide et la contrebande dans la catégorie des activités à haut risque. En conséquence, les autorités tunisiennes, y compris la CRF tunisienne, la Banque centrale, les autorités douanières et le Ministère de l'Intérieur, en partenariat avec le secteur privé (les banques et les bureaux de change), ont développé une plateforme nationale utilisant la technologie blockchain appelée Hannibal pour collecter, stocker et analyser en commun les données. La plateforme crée des tableaux de bord dynamiques pour mieux analyser les risques de BC/FT associés aux mouvements transfrontières d'argent liquide. Elle aide également les CRF, les organismes chargés de l'application de la loi, les banques et les bureaux de change à identifier et à détecter les réseaux de courriers d'argent liquide.

Le développement de systèmes automatisés utilisés pour évaluer les risques des entités surveillées, ainsi que de services en ligne pour



l'interaction avec le secteur privé, est une priorité des activités de contrôle de Rosfinmonitoring. L'Espace personnel sur son site web est une des solutions RegTech qui réunit plus de 60 000 organisations déclarantes (Entrepreneurs Individuels). Désormais, c'est un moyen de communiquer avec le Service et de transmettre des informations sur les personnes impliquées dans des activités terroristes et sur le financement de la prolifération, mais aussi un outil autonome de contrôle permettant d'accomplir un certain nombre de tâches visant à sensibiliser aux exigences légales et aux risques, même de changer le comportement de la personne contrôlée dans le domaine anti-blanchiment.

Les entités déclarantes reçoivent en ligne l'évaluation des risques établie sur la base des résultats de la surveillance à distance, ce système est un élément clé de ce mécanisme. L'efficacité de ces mesures correctives est assez élevée, parmi ces grands avantages on trouve la couverture, le coût réduit du point de vue de l'administration et la possibilité de personnaliser et de sélectionner de manière flexible les critères d'évaluation des risques. Grâce à cette coopération, chaque année des milliers d'entités déclarantes réduisent les risques de non-conformité aux exigences obligatoires en matière de LBC/FT. Le système permet non seulement de réduire le fardeau administratif sur les personnes contrôlées, mais aussi de redistribuer les ressources de l'organe de surveillance pour résoudre des tâches analytiques complexes qui requièrent un jugement professionnel et de l'expertise.

La fonctionnalité de l'Espace personnel est également orientée de façon à améliorer les connaissances des entités liées à la LBC/FT, leur sensibilisation aux exigences législatives, aux résultats de

ACTUELLEMENT, L'ESPACE PERSONNEL CONTIENT PLUS DE 60 TYPOLOGIES ACCOMPAGNÉES PAR DES SIGNES PERMETTANT DE LES IDENTIFIER.

On peut y trouver également la fonctionnalité d'apprentissage à distance, un certain nombre de cours de formation que l'utilisateur peut étudier puis évaluer ses connaissances à l'aide d'un test. Il est aussi possible de fournir automatiquement des explications sur les exigences légales pour des questions types.

l'évaluation nationale des risques, aux nouvelles tendances et aux schèmes d'activités illégales.

Dans le cadre du développement de mécanismes de communication avec le secteur privé, l'Espace personnel de la communauté professionnelle (associations, guildes) a été mis en service en 2022. Il permet, entre autres, de communiquer des détails relatifs à la conformité des organisations responsables avec les exigences de la législation LBC/FT, de notifier des événements et d'organiser la participation à ces événements pour les membres des communautés professionnelles concernées, etc.

Afin d'utiliser efficacement l'Espace personnel dans les procédures de CDD (vigilance à l'égard de la clientèle), un agrégateur d'informations sur le client contrôlé, provenant du plus grand nombre de sources possible, a été créé sous une forme unique et consolidée.

L'Espace personnel d'un organe de surveillance permet de consulter en ligne les résultats de surveillance à distance effectuée par Rosfinmonitoring, ce qui garantit que les organes de surveillance (supervision) dans le domaine de LBC/FT réagissent rapidement aux risques liés aux activités des entités contrôlées et facilite l'application d'approches uniformes pour la planification des activités de contrôle. En outre, cet Espace sert à fournir en ligne des macro-analyses permettant à l'organisme de surveillance de contrôler la dynamique des paramètres de respect de la loi du secteur et l'implication de ses représentants dans des transactions suspectes ainsi que son exposition à des risques spécifiques. Parmi les défis à venir, on planifie l'intégration dans l'Espace personnel du panel du chef de l'organe de surveillance.

Ce panel (établi pour la première fois pour les responsables des organes territoriaux de Rosfinmonitoring (figure 1)) présente des données analytiques supplémentaires

concernant, entre autres, l'efficacité des mesures de surveillance appliquées dans diverses sections analytiques (par instruments de contrôle, régions et types d'activités choisis). Ceci permet de corriger la fonctionnalité de l'équipe de surveillance en choisant les approches les plus efficaces pour les activités de contrôle.

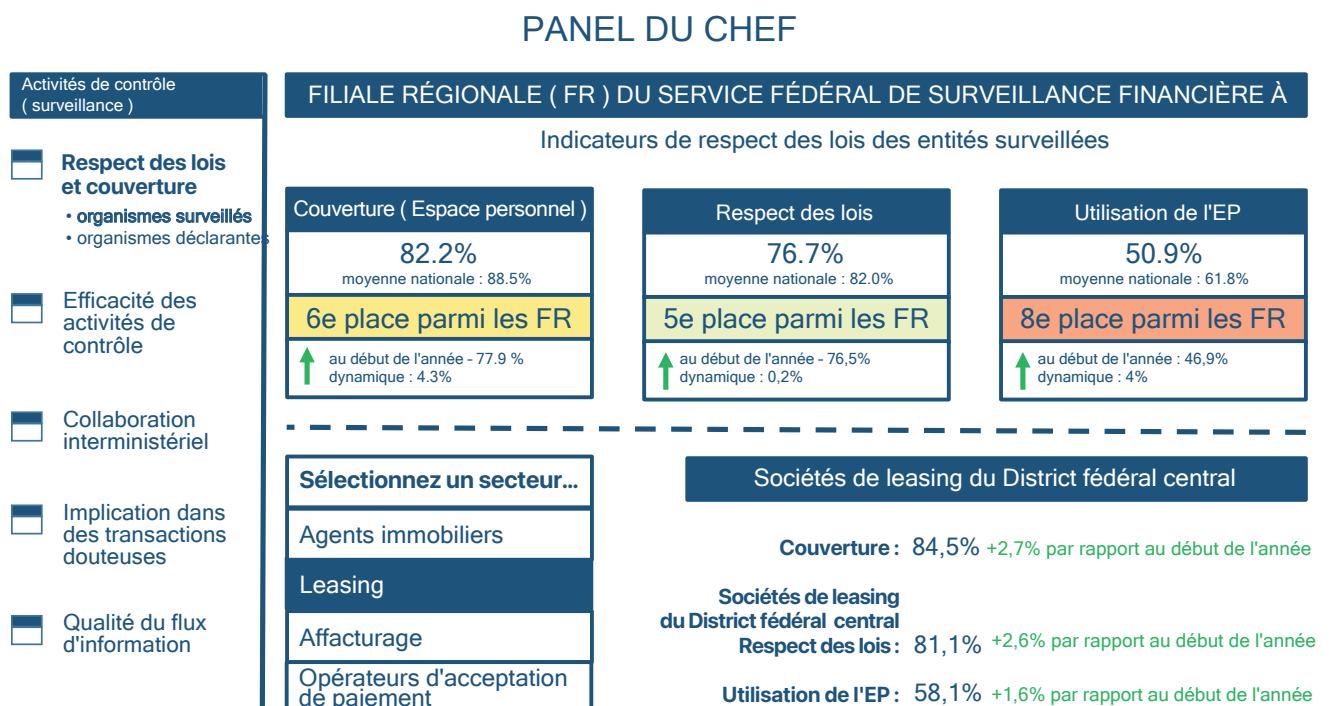
L'Espace personnel remplit également les fonctions de « feedback ». À partir de 2019, le feedback sur les déclarations de transactions suspectes (DTS) envoyées par les établissements de crédit est fourni aux entités responsables via l'Espace personnel sur le site web de Rosfinmonitoring sous la forme de l'Indice de qualité du flux d'informations (figure 2). Sur la base de certains algorithmes, se forme une évaluation des critères les plus importants caractérisant l'efficacité de l'interaction des informations entre les entités déclarantes et Rosfinmonitoring. Actuellement, les paramètres

d'interaction suivants sont évalués : rapidité des DTS, concentration des informations entrantes sur les risques réels, caractéristiques de l'interaction avec la CRF (envoi d'informations sur les risques (typologies), réponses aux demandes de la CRF, violation des délais de transmission des informations à la CRF).

Une évaluation intégrale caractérisant la qualité de l'interaction entre l'entité et la CRF est établie sur la base de ces critères. Comme résultats de ce format de feedback on obtient une efficacité accrue dans l'identification des transactions suspectes, une amélioration de la qualité des DTS et de leur ciblage sur les risques.

Une condition importante pour améliorer la qualité du flux d'informations provenant des acteurs responsables est l'orientation en temps utile des entités de surveillance financière vers les risques et les tendances actuels dans le domaine du crédit et de la finance.

► Figure 1. Panel du chef

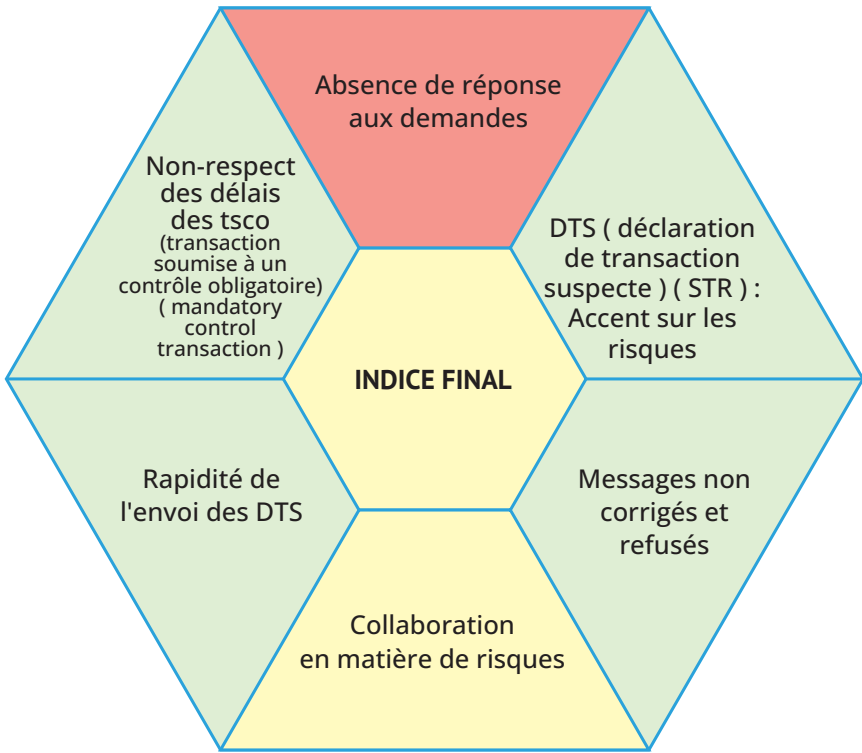


Un exemple de cette pratique est la fourniture de typologies et de signes de transactions suspectes aux établissements de crédit par le biais de la fonctionnalité de l'Espace personnel. Dans le contexte de la LBC/FT, la typologie se réfère à la manifestation de divers modèles de transactions suspectes utilisant l'infrastructure des établissements financiers qui sont systématiques ou récurrentes. La nature systémique est généralement liée à diverses vulnérabilités des systèmes de contrôle interne des entités faisant l'objet de surveillance financière primaire.

Les sources d'information sur les nouvelles typologies peuvent être les résultats d'analyse financière de la CRF et des entités qui font l'objet de surveillance financière. Par exemple, Rosfinmonitoring, en collaboration avec les établissements de crédit membres du Conseil de la conformité (un organe de consultation auprès de la Commission interministérielle pour LBC/FT), examine régulièrement des exemples d'analyse financière qui constituent souvent la base des typologies fournies par le biais de la fonctionnalité de l'Espace personnel. Il convient de noter qu'une telle communication des risques est également prise en compte dans la formation de l'Indice de qualité du flux d'informations.

L'analyse des informations reçues, y compris l'identifiant des typologies

► **Figure 2.** Indice de qualité du flux d'informations



(pour chacune desquelles un identifiant unique est attribué afin d'envoyer une DTS en cas d'identification d'une opération suspecte relevant d'attributs pertinents) permet à Rosfinmonitoring d'effectuer diverses modules thématiques en ligne, ce qui simplifie l'analyse du flux opérationnel.

En général, le développement de l'infrastructure informatique permet aux organes de surveillances d'accéder à un niveau supérieur de

fonctionnement grâce aux connaissances expertes élargies et à la prise de décision plus rapide.

L'objectif clé de ce développement dans le domaine de la surveillance pour l'avenir proche, c'est de promouvoir l'adoption de standards axés sur le client qui réduisent la charge réglementaire mais forment aussi un climat particuliers de partenariat et de confiance entre l'état et le secteur privé grâce à des communications plus ciblées.



REGISTRE DES BÉNÉFICIAIRES EFFECTIFS. EXPÉRIENCE DU KAZAKHSTAN

Conformément à l'Article 6-1 de la Loi de la République du Kazakhstan « Sur la lutte contre la légalisation (le blanchiment) de capitaux et le financement du terrorisme », l'Agence de surveillance financière de la République du Kazakhstan est autorisée à tenir le Registre des bénéficiaires effectifs des personnes morales (ci-après dénommé le Registre)



DINARA MOUSSINA,
Chef du Département d'analyse opérationnelle de l'Agence de surveillance financière de la République du Kazakhstan

Les informations et les données du Registre sur le bénéficiaire effectif de la personne morale sont fournies aux organismes suivants :

- 1) les autorités publiques de la République du Kazakhstan qui, dans les limites de leurs compétences, contrôlent si les entités chargées de la surveillance financière respectent la législation de la République du Kazakhstan relative à la lutte contre la légalisation (blanchiment) de capitaux et le financement du terrorisme, envers les entités dont ils sont responsables ;
- 2) les organismes chargés de l'application de la loi et les autorités publiques ;
- 3) les entités de surveillance financière.

Dans cet article, nous allons aborder les approches développées par l'Agence de surveillance financière, pour créer et tenir le Registre, ainsi

que ses fonctions réalisées dans l'espace personnel des organismes publics de régulation, des organismes d'application de la loi et des entités faisant objet de surveillance financière.

LES APPROCHES DE LA CRÉATION ET DE LA TENUE DU REGISTRE SONT MISES EN ŒUVRE SUR LA BASE DE 3 FACTEURS :

- les résultats de l'évaluation des risques des personnes morales, c'est-à-dire leur degré d'implication dans les infractions et le blanchiment de capitaux ;
- l'accès de l'Agence à diverses bases de données ainsi que la capacité informatique de les traiter ;
- les Recommandations du GAFI actualisées.

PROCESSUS COMMERCIAL DU REGISTRE DES BENEFICIAIRES EFFECTIFS

Selon la Recommandation du GAFI, « les informations sur les bénéficiaires effectifs doivent être complètes, exactes et à jour », c'est pourquoi l'étape la plus importante du processus commercial développé a été la collecte d'informations auprès de diverses sources.

Par conséquent, le début du processus commercial comprend la collecte d'informations sur les bénéficiaires effectifs déclarés par les personnes morales. Dans ce cas, les sources d'information sont les suivantes :

- **Ministère de la Justice** qui regroupe toutes les données d'enregistrement du pays ;
- **Entités de surveillance financière** qui sont chargés d'identifier et de noter les propriétaires bénéficiaires de leurs clients (Registre des gros actionnaires, Registre des bénéficiaires effectifs tenu par les participants du Centre International des Finances d'Astana) ;

- **Comité des recettes publiques** à qui dans le cadre de l'exécution des charges fiscales les résidents présentent des déclarations de contrôle des sociétés étrangères ;
- **Agence de surveillance financière** qui est habilitée à demander et à recevoir des informations sur les bénéficiaires effectifs ;
- **Ministère de l'énergie et ministère de l'industrie et du développement de l'infrastructure** qui sont des autorités compétentes à recevoir et à garder les informations sur les bénéficiaires effectifs des utilisateurs du sous-sol (norme internationale de transparence dans les industries extractives).

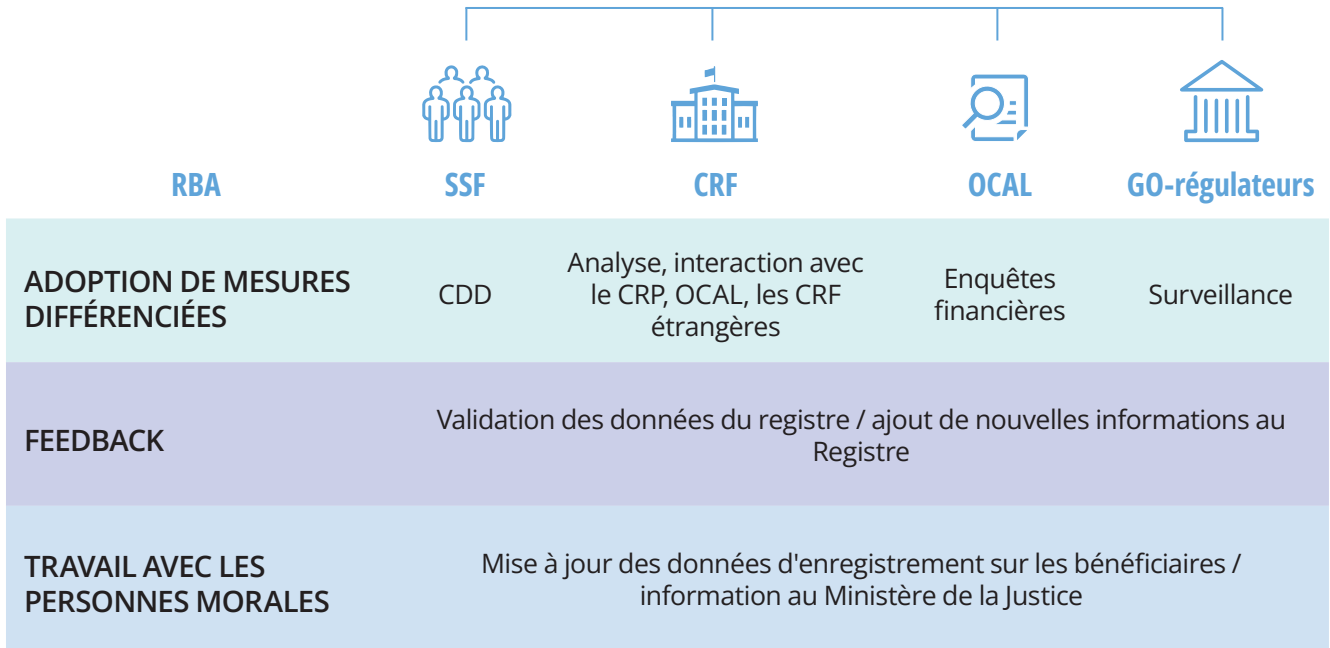
La première étape consiste donc à collecter auprès de plusieurs sources toutes les données déclarées par les personnes morales elles-mêmes sur leurs bénéficiaires effectifs.

La majeure partie de ces informations est disponible en ligne pour l'Agence de surveillance fiscale. Par conséquent, la collecte et la consolidation de données sont automatisées.

SOURCES DE DONNÉES SUPPLÉMENTAIRES

Afin de revérifier ces informations, des sources suivantes d'information supplémentaires sont collectées :

- messages sur les transactions suspectes et les transactions de seuil envoyés par les entités de surveillance financière ;
- Comité des recettes publiques: déclarations de revenus ;
- Ministère de la Justice: liens de parenté et relations professionnelles ;
- Comité des recettes publiques: factures électroniques ;
- informations des cellules étrangères de renseignement financier: historique des demandes ;
- sources de données ouvertes sur Internet.



STATUTS DES BÉNÉFICIAIRES EFFECTIFS

Une méthodologie détaillée d'algorithmes pour le traitement des données en vue de déterminer les relations avec les bénéficiaires a été développée sur la base de l'ensemble des informations. Les algorithmes de traitement des données sont automatisés. À ce jour, il s'agit de 19 algorithmes qui ont déjà été appliqués et dont l'efficacité a été

LE RÉSULTAT DES CALCULS DE CES ALGORITHMES EST L'ATTRIBUTION D'UN DES STATUTS SUIVANTS AUX PERSONNES PHYSIQUES :

- « Bénéficiaire effectif enregistré »
- « Bénéficiaire effectif présumé »

démontrée.

Si l'information à propos des propriétaires est présentée au Ministère de la Justice, ces bénéficiaires sont reconnues comme « enregistrés », les autres sont considérées comme « présumés ».

Chaque algorithme de détermination du « bénéficiaire effectif présumé » utilise une méthodologie et une source d'information différentes, et il a son propre poids et son propre score de crédibilité. Aujourd'hui, la crédibilité est évaluée par un expert sur une échelle de 1 à 4, où 1 correspond à une faible probabilité de crédibilité et 4 à une forte probabilité de crédibilité.

Chaque algorithme s'exécute selon l'horaire convenu. Les résultats de



Les utilisateurs du Registre sont les membres du système de lutte contre le blanchiment d'argent : autorités publiques de régulation, organismes chargés de l'application de la loi, entités de surveillance financière, cellules de renseignement financier.

COMPTE TENU DU TRAVAIL SPÉCIALISÉ EFFECTUÉ, L'UTILISATEUR DU REGISTRE A LA POSSIBILITÉ D'INSCRIRE SON OPINION DANS LE REGISTRE DES BÉNÉFICIAIRES EFFECTIFS PRÉSUMÉS, C'EST-À-DIRE :

1. confirmer ou non l'hypothèse de la cellule de renseignement financier
2. ajouter son hypothèse : bénéficiaire effectif présumé supplémentaire avec la description de son algorithme/projet.

chaque période de fonctionnement des algorithmes sont enregistrés.

Tout feedback de la part d'un membre du système de lutte contre le blanchiment de capitaux est précieux et contribue à l'amélioration et à l'extension des 19 algorithmes actifs.

En outre, dans le cadre du travail spécialisé avec les clients, avec les objets d'analyse, avec les objets de contrôle, les utilisateurs stimulent la mise à jour des données d'enregistrement par les personnes morales elles-mêmes.

Ainsi, en utilisant activement le Registre des bénéficiaires effectifs dans ses activités, chaque membre du système de lutte contre le blanchiment de capitaux contribue à notre cause commune qui est de prévenir et d'empêcher l'implication des personnes morales dans les infractions et le blanchiment de capitaux.



LE PRÉSENT ET LE FUTUR DE L'INTELLIGENCE ARTIFICIELLE ET DES TECHNOLOGIES FINANCIÈRES

35 SVETLANA ORLOVA :

« Les produits et solutions numériques sont des étapes décisives vers le développement de l'audit des finances publiques »

39 V. L. DOSTOV

L'intelligence artificielle dans la finance et son impact sur certains aspects de la LBC/FT

43 MIKHAÏL PRONINE

Application de l'intelligence artificielle pour la surveillance financière

46 ALEXEÏ GUELETA :

« Le marché de la technologie financière de Russie est un des plus innovants et avancés dans le monde entier »

SVETLANA ORLOVA :

« LES PRODUITS ET SOLUTIONS NUMÉRIQUES SONT DES ÉTAPES DÉCISIVES VERS LE DÉVELOPPEMENT DE L'AUDIT DES FINANCES PUBLIQUES »



Svetlana Orlova, auditrice de la Chambre des comptes de la Fédération de Russie, a parlé aux rédacteurs de la revue « Sécurité Financière » des mesures visant à introduire l'intelligence artificielle dans le domaine du contrôle de l'État (audit), des possibilités offertes par les nouvelles technologies pour améliorer l'administration publique, ainsi que des solutions numériques actuelles dans ce domaine particulier

Madame Orlova, merci d'avoir trouvé le temps de nous parler malgré votre agenda chargé. Cette édition est consacrée, entre autres, au développement de l'intelligence artificielle. À votre avis, comment les capacités de l'IA peuvent-elles être mises en service dans le domaine du contrôle des finances publiques (audit) ?

Tout d'abord, je tiens à préciser que nous travaillons dans la direction indiquée par le président russe Vladimir

Poutine pendant le Forum économique international de Saint-Petersbourg en juin 2023. On pourrait la résumer ainsi : « Un domaine clé de l'économie de l'offre concerne l'automatisation active et la maîtrise de technologies d'intelligence artificielle. Il faut mettre en œuvre et utiliser activement ces développements, soutenir la préparation de logiciels nationaux dans le domaine de données massives, lancer des projets dans le domaine de l'intelligence artificielle ».

En février 2024, le Président de la Fédération de Russie a apporté des modifications importantes à la Stratégie nationale pour le développement de l'intelligence artificielle jusqu'à 2030. En particulier, les organes fédéraux du pouvoir exécutif (OFPE) doivent suivre les dispositions de cette stratégie lors de l'élaboration et de l'introduction des documents de planification stratégique sectorielle. Ainsi, après les changements introduits, les activités des OFPE seront, en quelque sorte,

orientées vers les technologies de l'intelligence artificielle.

Cette ligne stratégique a été de nouveau soulignée dans le message du Président de la Fédération de Russie à l'Assemblée fédérale. La Chambre des comptes y travaille depuis quelques années. Tout d'abord, sur la numérisation des activités des inspecteurs.



Bien sûr, il y a quelques technologies d'IA qui sont déjà utilisées dans les smartphones, la médecine, l'éducation, les systèmes de maisons intelligentes et l'industrie.

Les éléments importants nécessaires à la création et à l'utilisation des technologies d'intelligence artificielle sont les données massives et la capacité à les analyser à l'aide de technologies de réseaux neuronaux.

Dans le domaine de l'audit (contrôle) des finances publiques, des éléments mentionnés de l'intelligence artificielle, la qualité des données massives et surtout leur intégrité ont une importance particulière. C'est sur l'organisation de l'analyse des données massives que nous avons d'abord porté notre attention. Ce problème a été en grande partie résolu dans le cadre des solutions numériques élaborées par

la Cour des comptes à l'aide d'outils numériques pour la collecte, l'analyse et la visualisation des données (analyse des données). À la fin de l'année 2023, le registre des solutions et produits numériques de la Cour des comptes contient des données sur plus de 300 solutions et produits numériques.

Ces solutions font passer l'audit au niveau supérieur grâce à des technologies et des techniques modernes.

En outre, les solutions numériques réduisent d'au moins un tiers le temps que l'inspecteur consacre à analyser les données de l'objet de l'audit (contrôle). En minimisant le facteur humain, le risque d'erreurs est presque inexistant. Troisièmement, l'éventail des informations à vérifier a été considérablement élargi.

Bien sûr, cela n'aurait pas été possible sans travail sur la transformation numérique de l'audit réalisé à la Cour des comptes.

Dans le cadre du domaine d'audit de l'administration publique dont je suis responsable, nous facilitons la transformation numérique de nos objets d'audit également.

Madame Orlova, étant donné qu'il existe déjà des résultats de travaux dans ce domaine, je vous demanderais d'en parler plus précisément.

À titre d'exemple, je peux citer le travail commun sur l'introduction des technologies modernes de l'information dans les procédures légales.

En 2023, nous avons organisé 4 réunions élargies avec 15 ministères et agences leaders dans le domaine de la numérisation, dont le Ministère du développement numérique, des communications et des médias de la Fédération de Russie, le Ministère de la Justice, le Trésor Fédéral, le Service Fédéral des Impôts, le

Service fédéral des huissiers de justice, Rosimushchestvo (Agence fédérale pour la gestion de biens publics) et d'autres agences. Nous avons discuté avec eux des bonnes pratiques en matière d'introduction des technologies modernes de l'information dans les procédures légales, de la coopération interdépartementale entre les autorités publiques et le système judiciaire, y compris l'amélioration du travail avec les comptes de dépôt des tribunaux de commerce.

Nous avons discuté ces questions lors d'une réunion avec des collègues du Gouvernement de la Fédération de Russie, de la Cour suprême de la Fédération de Russie et du Conseil de la Fédération de l'Assemblée fédérale de la Fédération de Russie.

À la fin de 2023, avec notre participation, le Département judiciaire auprès de la Cour suprême de la Fédération de Russie, le Ministère du développement numérique de Russie et le Trésor fédéral ont conclu un accord d'intention visant à développer des approches communes pour introduire des technologies modernes de l'information et de la communication dans les procédures légales et la gestion des dossiers de la procédure légale.

Le résultat de cette collaboration devrait être la création d'un service pratique pour les citoyens et les entreprises, inclus dans la procédure judiciaire, qui simplifiera le dépôt de fonds par les parties aux procédures judiciaires, augmentera la transparence de leur mouvement et réduira à néant l'abus de ces fonds.

Des solutions techniques sont en train d'être élaborées pour ce projet et nous pensons que sa mise en œuvre pilote pourrait commencer prochainement au sein du Tribunal de commerce de Moscou.

En cas de validation réussie des mesures stipulés par l'accord, il est prévu de les appliquer dans tous les tribunaux fédéraux et les directions du Département judiciaire auprès de la Cour suprême de la Fédération de Russie et toutes les entités de la Fédération de Russie.

» **« LE RÉSULTAT DE CETTE COLLABORATION DEVRAIT ÊTRE LA CRÉATION D'UN SERVICE PRATIQUE POUR LES CITOYENS ET LES ENTREPRISES, INCLUS DANS LA PROCÉDURE JUDICIAIRE, QUI SIMPLIFIERA LE DÉPÔT DE FONDS PAR LES PARTIES AUX PROCÉDURES JUDICIAIRES, AUGMENTERA LA TRANSPARENCE DE LEUR MOUVEMENT ET RÉDUIRA À NÉANT L'ABUS DE CES FONDS »**

En outre, avec le soutien des représentants du système judiciaire, le Département judiciaire de la Cour suprême de la Fédération de Russie, ainsi que les ministères et les agences, une position commune est en cours d'élaboration sur la formation d'une « feuille de route » pour la réalisation de solutions numériques à la fois dans les procédures légales et dans la coopération interdépartementale.

Plusieurs projets pilotes devraient être lancés avec notre participation directe :

- le système judiciaire, en collaboration avec le Ministère du développement numérique, le Ministère de la Justice, le Ministère des Finances, le Trésor, le Service fédéral des impôts et les huissiers de justice travaille

à résoudre le problème actuel – **attribution d'identificateurs uniques de paiement (IUP)** dans les titres exécutoires rendus par les tribunaux. Une solution temporaire a été trouvée, mais il reste encore beaucoup à faire pour synchroniser le travail de toutes les parties concernée dans ce domaine ;

- le système judiciaire, le trésor et les huissiers de justice travaillent à l'établissement d'un grand projet commun qui est très important – la mise en place d'un modèle de registre pour l'exécution de décisions judiciaires. Le modèle vise à assurer la transparence des procédures d'exécution et facilitera une coopération électronique plus efficace entre les autorités publiques et les citoyens.

Madame Orlova, pouvez-vous donner des exemples concrets de solutions numériques et de leurs résultats positifs pour l'amélioration de l'administration publique ?

Le secteur dont je suis responsable a réalisé 18 solutions numériques (produits) pour la seule année 2023.

Je voudrais parler des solutions les plus importantes, dont les résultats ont eu un impact positif sur l'amélioration de l'administration publique.

Ainsi, afin de mettre en œuvre les Recommandations méthodologiques sur l'identification et l'évaluation des risques de corruption dans le cadre des activités de contrôle, d'expertise et d'analyse utilisant la technologie de l'intelligence artificielle, un produit numérique « Identification des risques de corruption dans le cadre d'achats effectués auprès d'un seul fournisseur » a été développé.

Le produit permet d'analyser automatiquement la conformité du contrat aux dispositions de la Loi fédérale « Sur le système contractuel dans le domaine de l'acquisition de biens, de travaux et de services pour les besoins de l'État et des municipalités » avec la réglementation d'achat auprès d'un fournisseur unique et, s'il existe une non-conformité aux dispositions de la loi, il montre le risque d'infractions.

Lors du développement du produit, le modèle a analysé environ 100 000 contrats enregistrés dans le SIU (Système d'Information Unifié) et les variantes possibles de leurs formulations, ce qui lui permet d'identifier des écarts et des risques éventuels.

À ce jour, le projet est achevé et a été mis en ligne sur le portail de la Chambre des comptes.

Identification des risques de corruption dans le cadre d'achats effectués auprès d'un seul fournisseur

The screenshot shows the interface of the digital tool for identifying corruption risks. It features a document titled 'Identification des risques de corruption lors du contrôle des marchés publics au titre de l'alinéa 1 de l'Article 93 44-FZ'. Annotations with red boxes and arrows point to specific elements: 'Veuillez saisir le texte du contrat (considérants et objet)' points to the contract text input field; 'Cliquez sur « Vérifier »' points to the 'Vérifier' button; 'Résultat d'analyse' points to the analysis results section; and 'Possible violation ou type de econtrat inconnu' points to a specific risk identified by the system. To the right, a list of findings is shown, including violations previously unidentified and a significant reduction in verification time from 25 hours to 15 minutes.

Veuillez saisir le texte du contrat (considérants et objet)

Cliquez sur « Vérifier »

Résultat d'analyse

1. Les violations que l'inspecteur ignore (auparavant pratiquement non identifiées) sont révélées au niveau de **80-90%**
2. Le temps de vérification de chaque contrat du marché public est réduit environ **100 fois** – de 25 heures de travail à 15 minutes

Possible violation ou type de econtrat inconnu

Use of digital solutions in identifying corruption risks

Par ailleurs, une solution numérique très intéressante a été développée au cours des activités d'analyse et d'expertise « Analyse de l'administration des comptes personnels (comptes de dépôts) pour enregistrer les transactions avec les fonds qui étaient temporairement à la disposition des tribunaux de commerce de 2012 à 2022 et pendant la période écoulée de 2023 ».

L'objectif principal de la solution numérique est de comparer les documents de paiement pour les fonds reçus à la disposition temporaire des tribunaux de commerce avec le nombre d'affaires acceptées pour examen pendant 11 ans, et de vérifier l'application des dispositions du Règlement sur l'organisation des activités des tribunaux fédéraux et des directions du Département judiciaire dans les entités constitutives de la Fédération de Russie sur le travail avec des comptes personnels (comptes de dépôts) pour enregistrer les transactions avec des fonds temporairement à disposition.

Et maintenant, les données brutes : nombre de titres de paiement – environ 9 millions ; nombre de procédures d'arbitrage – plus de 27 millions.

Il est difficile d'imaginer le nombre d'inspecteurs et le temps qu'il faudrait pour traiter et analyser cet ensemble d'informations et de chiffres.

En même temps, nous avons rencontré des difficultés, dans le fait que les données étaient caractérisées par une incertitude significative : les fonds avaient été déposés par certaines personnes, mais auraient pu être payés à d'autres personnes, y compris celles qui n'étaient pas impliquées dans la procédure judiciaire, les données concernant les fonds reçus sur le compte de dépôt du tribunal étaient incomplètes (où le NIF de la Direction du Trésor fédéral était indiqué au lieu du NIF du tribunal).



La solution numérique développée a aidé à résoudre ce problème.

Et voici le plus important :

- sur la base des résultats de ces activités, le besoin de réaliser un projet pilote visant à optimiser et à automatiser les processus de gestion des fonds sur les comptes personnels ouverts auprès des organismes du Trésor fédéral déposés par les citoyens et les entités conformément à la législation en matière de procédure pénale, a été confirmé ;
- on a proposé de modifier le Règlement de l'organisation des activités des tribunaux fédéraux et des directions du Département judiciaire dans les entités territoriales de la Fédération de Russie pour travailler avec des comptes personnels (comptes de dépôts) afin de comptabiliser les transactions avec des fonds mis à disposition temporaire.

Sur quelle solution numérique vos employés travaillent-ils actuellement ?

Aujourd'hui, après avoir reçu le feedback de plusieurs départements de la Cour des comptes, nous mettons au point la solution numérique développée dans le cadre de la réalisation de nos Recommandations méthodologiques pour identifier et évaluer les risques de corruption.

La solution est mise au point à l'aide d'une nouvelle technologie, appelée l'intelligence artificielle « génératrice ».

Pour ceux qui n'ont pas encore rencontré ce problème, je m'explique : cette technologie implique la possibilité d'apprendre son propre algorithme de recherche d'informations en fonction de critères définis.

Une fois la solution finalisée et testée, les résultats d'analyse du marché public indiqueront non seulement les zones de risque possibles, mais aussi la description du risque et l'ensemble des causes pour lesquelles les risques d'une éventuelle violation ont été identifiés.

En outre, lorsque le projet sera prêt, nous serons en mesure d'analyser les contrats sélectifs, mais aussi nous prévoyons de télécharger les dossiers dans n'importe quel format compatible avec la machine.

L'identification automatisée des zones à risque réduira considérablement le temps nécessaire au traitement et à l'analyse des documents.

Je tiens à préciser qu'aucune intelligence artificielle ne remplacera le travail d'un inspecteur et ne peut être que son assistante.

» « JE TIENS À PRÉCISER QU'AUCUNE INTELLIGENCE ARTIFICIELLE NE REMPLACERA LE TRAVAIL D'UN INSPECTEUR ET NE PEUT ÊTRE QUE SON ASSISTANTE »

L'INTELLIGENCE ARTIFICIELLE DANS LA FINANCE ET SON IMPACT SUR CERTAINS ASPECTS DE LA LBC/FT



> VICTOR DOSTOV,
Président du Conseil AAMMETF
(Association des acteurs du marché
de la monnaie électronique et du
transfert de fonds), docteur en sciences
physiques et mathématiques, chargé de
recherche de l'Université des finances

L'intelligence artificielle est probablement la percée technologique la plus importante des deux dernières années. Il ne fait aucun doute qu'un saut qualitatif dans son développement nous permettra de réévaluer les approches traditionnelles de la résolution de nombreuses tâches intellectuelles qui exigeaient auparavant une participation humaine et d'élargir la gamme des tâches qui peuvent être résolues sans participation humaine

Selon un récent rapport consultatif de la Banque Centrale de la Fédération de Russie¹, le secteur financier est devenu l'un des consommateurs les plus actifs de la nouvelle technologie. Dans cet article, nous essayons très brièvement d'examiner l'essence de cette percée technologique et son impact possible sur le développement du secteur, en accordant une attention particulière aux aspects de la LBC/FT.

INTRODUCTION À LA TECHNOLOGIE

Il est impossible de présenter d'une manière exhaustive dans le cadre d'un article une technologie aussi vaste que l'IA, dont le développement et l'utilisation comptent plusieurs années. Nous nous limiterons à formuler les points essentiels liés aux réseaux principaux de neurones et aux modèles de langage LLM (Large Language Models) basés sur

ces réseaux. Le mot « linguistique » ne doit pas être trompeur car tout objet traduit en une séquence de zéros et de uns que ce soit un livre, une photo numérique, des données de notation, des graphiques de paiement de crypto-monnaie ou des fluctuations de leurs change, des vidéos et d'autres, du point de vue pour l'IA représente des énonciations en langages spécialisées.

¹ <https://cbr.ru/press/event/?id=17177>.



De manière très simple, un réseau neuronal est une séquence de transformations de colonnes de valeurs initiales (vecteurs) en un vecteur de résultat final. Par exemple, un LLM typique prend le texte source, c'est-à-dire une colonne (ou plus couramment, une ligne) de caractères alphabétiques et les transforme en une colonne (ligne) à la sortie. L'IA considère également le texte de cet article comme une longue colonne de lettres. On peut le soumettre à l'entrée de l'IA en ajoutant une colonne de questions et obtenir une réponse simple Oui/Non, une réponse plus détaillée ou une traduction vers une autre langue. On peut représenter de nombreux objets sous la forme d'une colonne de caractères, par exemple une image, une vidéo, des données issues d'une expérience scientifique, des ensembles de transactions, etc.

La conversion elle-même est élémentaire (exemple d'image). Nous prenons la première colonne, la transformons en une deuxième selon une règle simple : chaque cellule dans la colonne résultante est la somme de toutes les valeurs de la première colonne multipliée par les coefficients arbitraires de l' A_{ij} formant la table (matrice). Ensuite, les valeurs obtenues dans chaque cellule de la deuxième colonne sont transformées au moyen de formules qui diminuent les petites valeurs et augmentent les grandes, ce qui accroît, pour ainsi dire, le contraste du résultat. Ensuite, à partir de la deuxième colonne, on passe à la troisième en utilisant la même règle à l'aide de la matrice suivante A_{ij} etc. jusqu'à la colonne de réponse. La matrice des coefficients, la formule de transformation et la colonne forment une couche. Le nombre de couches nécessaires est étonnamment faible. Par exemple, en 1958 Rosenblatt a montré qu'un réseau neuronal à trois couches

est suffisant pour toute tâche de classification d'images (reconnaître des chiffres et des lettres, distinguer des voitures et des piétons, et bien d'autres tâches).

D'où l'IA prend-elle les matrices A_{ij} ? Là aussi, c'est facile : l'apprentissage est requis. Ce processus est simple. Tout d'abord, les coefficients sont choisis au hasard et l'IA se voit présenter une ligne d'entrée dont la réponse est connue, par exemple une question pour laquelle on sait si c'est Oui ou Non. Au début l'IA produit une réponse d'une manière aléatoire. Si elle a deviné, on lui pose la question suivante. Si elle ne devine pas, la matrice est légèrement modifiée et la question est répétée, puis modifiée à nouveau et répétée jusqu'à l'obtention d'une réponse correcte. Cette sélection est répétée plusieurs fois jusqu'à ce que la bonne réponse soit obtenue pour la grande majorité du temps (ou toujours). L'IA est ensuite considérée comme avoir passé l'apprentissage et elle est introduite dans la vie réelle pour répondre à de nouvelles questions.

L'humanité a longtemps rêvé de créer une intelligence artificielle. En ce qui concerne les modèles de langage, les premières idées ont été proposées par le mathématicien russe Markov en 1913. Toutefois, ce n'est que vers 2022 qu'une masse critique de capacités logicielles, matérielles et contextuelles rendant possible l'apprentissage de l'intelligence artificielle puissante a été accumulée et que des modèles de traitement du texte et de l'image ont commencé à émerger rapidement.

En même temps, il s'est avéré que les LLM basés sur les réseaux

neuraux ont la propriété d'être polyvalents. L'IA a été toujours développée dans de nombreux domaines relativement indépendants les uns des autres. Les algorithmes utilisés pour analyser les textes étaient très différents de ceux utilisés pour les jeux ou le contrôle des drones. Les réseaux neuronaux d'apprentissage en profondeur sont omnivores, ils ont réussi à résoudre tous les problèmes transformés en vecteurs de données. Cela a permis d'échapper à la dispersion des ressources et de se concentrer sur un domaine révolutionnaire. L'utilisation de l'IA a immédiatement commencé à diffuser dans un grand nombre de domaines de l'activité humaine, de l'art numérique à la médecine. Bien sûr, la finance ne font pas exception.

L'IA DANS LA FINANCE

En raison de l'accent mis initialement sur les modèles de langage, les mises en œuvre les plus rapides ont été liées à la communication avec la clientèle. Ceux-ci comprennent les chatbots de service clients, l'analyse des demandes, le contrôle de travail du personnel des centres d'appels, etc. Cela comprend également, par exemple, l'optimisation des descriptions de produits. Ici, des modèles de langage communs sont utilisés, les subtilités financières n'apparaissent que dans le contexte.

L'utilisation de l'IA pour optimiser les produits eux-mêmes repose également sur l'analyse du comportement des clients. Dans ce cas, l'apprentissage porte sur une série de paramètres différents relatifs aux produits, tels que le dépôt, et l'IA est formée pour optimiser ces paramètres afin d'obtenir le résultat souhaité, par exemple, atteindre un certain niveau des ventes. Des tentatives plus ambitieuses ont été

faites pour analyser et optimiser le comportement des clients en général mais, il est apparu que ce comportement est mal géré.

Une direction distincte est le scoring. L'IA permet d'évaluer les clients sur la base d'approches non triviales et de liens entre différents paramètres, ce qui permet, par exemple, d'accorder des prêts avec plus de succès.

De grands espoirs reposent sur l'utilisation de l'IA dans la sécurité de l'information des banques. Toute demande externe adressée à un système bancaire automatisé (SBA) peut être considérée par l'IA comme provenant d'un client légitime ou comme une cyberattaque. L'objet de l'apprentissage est constitué d'un grand nombre d'enregistrements historiques avec une répartition des demandes de bonne foi et des tentatives d'attaque.

Il s'agit d'une liste très courte d'exemples qui ne cesse de croître en termes de diversité de segments d'application.

IA ET LBC/FT

Les analystes ont attiré l'attention sur l'importance pratique de l'utilisation de l'IA dans la LBC/FT il y a déjà longtemps. En 2018, KPGM et l'Association des experts certifiés dans la lutte contre le blanchiment d'argent (ACAMS) ont constaté une accélération considérable de la mise en œuvre de l'IA dans cette lutte. Le GAFI l'a également souligné dans sa note analytique². À ce moment, les principaux domaines d'intervention sont les suivants :

1. Analyse du risque client lors de la mise en service

Dans ce cas, l'IA est formée sur une grande base de données d'anciens

clients bancaires (personnes morales et physiques) dont la qualité est connue à posteriori. L'apprentissage vous permet de classer les clients en fonction du risque de manière beaucoup plus efficace, ce qui résout, dans une large mesure, le problème du dérisquage. Selon Sber et HSBC, ils parviennent ainsi à fournir des services à une grande partie des clients qui ont reçu des refus non motivés au cours de la procédure d'examen traditionnelle.

2. Analyse des opérations courantes

L'analyse classique des transactions s'appuie sur des modèles déterminés, tels que les paiements fractionnés, la consolidation, l'utilisation d'intermédiaires suspects, etc. Toutefois, les schémas réels sont souvent plus sophistiqués et ne relèvent pas de l'analyse formelle. L'IA vous permet d'échapper aux limites des critères formels, de suivre et de signaler plus efficacement les transactions suspectes. Ces méthodes sont déjà utilisées par VTB, Sber, Standard Chartered, JPMorgan Chase, Danske Bank et d'autres. Il convient de noter que ces mécanismes sont également efficaces pour contrôler les systèmes de paiement distribués. En particulier, dès août 2020, Rosfinmonitoring a fait part du développement d'un prototype de système d'analyse des transactions de crypto-monnaie basé sur la technologie de l'intelligence

artificielle. Le système a été appelé « Blockchain transparente » et a été mis en service en février 2021.

3. Construction de graphes d'affiliation

La tâche technique la plus importante en matière de LCB/FT consiste à trouver les liens cachés d'intérêt et d'affiliation entre les participants à des structures de paiement complexes. L'IA permet d'analyser à la fois les transactions et les informations externes (inscriptions dans les Registres des personnes morales, renseignements sur les propriétaires provenant de sources externes, etc.) pour construire des graphes dont les ensembles contiennent des personnes morales et physiques et dont les liens entre les ensembles reflètent le degré d'affiliation. Compte tenu de ce qui précède, les relations formelles et informelles entre des participants apparemment indépendants aux transactions de paiement sont identifiées avec succès.

4. Surveillance de la conformité humaine

Ce modèle a d'abord été testé sur les centres d'appel « humains » (par exemple, les solutions JustAI). Il existe aujourd'hui un certain nombre de problèmes de client qui ne peuvent pas être résolus par l'IA. Cependant, en analysant les textes et les dialogues vocaux, elle peut faire des évaluations et des



² Opportunities and challenges of new technologies for AML/CFT <https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Opportunities-Challenges-of-New-Technologies-for-AML-CFT.pdf.coredownload.pdf>.



recommandations sur la qualité de travail du personnel. De la même manière, l'IA peut contrôler la performance de la conformité « humaine », en repérant les erreurs type, en classant le personnel en fonction de la qualité de son travail et en formulant les recommandations appropriées.

5. Analyse des changements à la législation

Certains espoirs sont placés sur l'utilisation de l'IA dans le traitement automatisé des documents réglementaires ce qui permettrait potentiellement d'optimiser les politiques internes de la banque lorsque les exigences du régulateur changent.

6. Analyse des contrats

Dans le cadre des activités de conformité, un temps important est consacré à l'analyse des documents fournis pour confirmer l'origine des fonds et l'objectif de la transaction. Il s'agit d'une charge assez importante, en raison de la spécificité et de la diversité de ces documents. L'IA est capable d'analyser ces documents pour s'assurer qu'ils sont authentiques et qu'ils correspondent à l'objectif de la transaction.

7. Construire des paramètres de base

Comme nous l'avons vu plus haut, l'IA peut modifier le modèle de conformité en passant d'un ensemble fixe de critères à l'analyse d'un ensemble complet d'opérations. L'inverse est également possible : vous pouvez former l'IA à un ensemble de transactions douteuses, en lui demandant de sélectionner l'ensemble limité de critères le plus efficace pour procéder à une analyse rapide.

8. Identification

Un bloc distinct de tâches est associé à l'identification du client. Ces tâches ne sont pas spécifiques au secteur financier et sont plutôt liées à l'objectif général d'identification de la personne. Cela inclut l'analyse des

photos et des documents des clients, l'analyse des enregistrements vocaux et vidéo et toute autre technique permettant d'accroître l'authenticité de l'identification du client, que ce soit à distance ou en personne.

VULNÉRABILITÉS DE L'IA PAR RAPPORT À LBC/FT

Malgré tous ses avantages, l'IA présente des spécificités qui comportent une menace potentielle dans toute application, et en particulier dans la finance. Contrairement aux approches algorithmiques qui permettent d'analyser la prise de décision de l'IA, un réseau neuronal ne permet pas, en principe, d'être interprété en termes d'algorithme. Nous ne pouvons pas, par exemple, lors de l'analyse de transactions suspectes, identifier les parties des matrices Aij responsables de la recherche de fractionnement et de consolidation, etc. Par conséquent, nous ne pouvons tester la fiabilité de fonctionnement de l'algorithme que statistiquement, en lui donnant un grand nombre de tâches et en vérifiant la qualité d'exécution. Même dans ce cas, il existe un certain nombre de problèmes typiques, comme les suivants :

- hallucinations, lorsque, sur la base de données correctes, l'IA crée des artefacts qui n'ont aucun rapport avec la réalité. Dans certains cas, l'IA a inventé des précédents judiciaires ou proposé des réductions inexistantes.
- champs de mines, lorsque l'IA donne des réponses absolument incorrectes avec une légère modification des données initiales. La nature de ce phénomène n'est pas définitivement comprise, ce qui le rend difficile à contrer.
- réapprentissage, lorsque l'augmentation du volume et de la qualité des données d'entrée entraîne inexplicablement une

dégradation de la qualité des réponses et un certain nombre d'autres problèmes.

Un moyen relativement efficace consiste à utiliser des systèmes à composantes multiples dans lesquels un réseau neuronal vérifie les résultats d'un autre. Néanmoins, il n'existe pas aujourd'hui de solution définitive à ces problèmes.

UTILISATION DE L'IA POUR LE BC/FT

Bien entendu, un outil aussi puissant a inévitablement attiré l'attention de la communauté criminelle. Nous ne disposons pas encore d'un typage des applications de l'IA pour le blanchiment de capitaux ou le financement du terrorisme, mais nous pouvons envisager avec une certaine confiance les possibilités suivantes : utilisation de bots pour communiquer avec les banques dans le cadre de l'embarquement, fabrication de fausses pièces d'identité, simulation d'identités dans le cadre de l'identification à distance, optimisation de scripts pour l'ingénierie sociale, optimisation des graphes de transactions criminelles, etc. Ce sujet mérite un article séparé.

On ne doute pas que l'IA trouvera des applications efficaces dans le secteur bancaire en général et dans la LBC/FT en particulier. L'auteur estime que les capacités pratiques de l'IA sont aujourd'hui exagérées et que bientôt elles seront complètement réévaluées. Néanmoins, l'analyse des capacités de l'IA et l'élaboration de méthodologies pour lutter contre les utilisations criminelles de l'IA devraient être une priorité pour les analystes et les praticiens dans le domaine de LBC/FT.

APPLICATION DE L'INTELLIGENCE ARTIFICIELLE POUR LA SURVEILLANCE FINANCIÈRE

Aujourd'hui, l'application d'intelligence artificielle est devenu un courant dominant dans tous les domaines. En même temps, le secteur bancaire est souvent une sorte de moteur de la promotion de nouveaux produits et de solutions informatiques avancés



> MIKHAÏL PRONINE,
Vice-président, chef du Département
de surveillance financière de la
banque PSB, docteur en sciences
économiques

Nous observons un grand nombre de solutions efficaces dans le domaine des prêts, des services liés aux transactions à la clientèle et, en particulier, dans les domaines où l'expertise repose en grande partie sur l'analyse automatisée des données et du comportement des clients.

Dans cette logique, on a l'impression que le domaine de lutte contre le blanchiment, concentré sur la détection des activités suspectes des clients, est idéal à l'application d'outils d'apprentissage machine, l'un des sous-ensembles de l'intelligence artificielle.

Dans le cadre du travail analytique de l'unité de surveillance financière de la banque PSB, nous avons commencé à expérimenter l'utilisation d'outils d'apprentissage automatique en 2020. L'accent a été mis sur les différents modèles mathématiques permettant de détecter les anomalies dans le comportement de paiement des clients.

Certains résultats de qualité ont été obtenus en utilisant un algorithme combinant un arbre de décision et une régression logistique. Cependant, malgré le temps considérable passé

à la recherche, le fonctionnement de ce modèle n'est jamais été beaucoup plus efficace que le travail des experts-analystes.

Par contre, nous avons acquis une expérience importante qui nous a permis de définir une stratégie d'action.

Tout d'abord, nous avons identifié une tendance intéressante. Dans la plupart des cas, le comportement de paiement des clients suspects n'est pas inhabituel par rapport à la clientèle. En effet, les clients suspects doivent constamment « s'adapter » pour ne pas être découverts.

Cette adaptation et cette imitation du comportement normal des clients honnêtes aboutit à ce que les modèles mathématiques ne classent pas comme inhabituel le comportement des clients qu'on soupçonne, mais le comportement de la partie des clients honnêtes qui ne se comportent pas d'une manière habituelle. Cette spécificité est caractéristique, par exemple, des jeunes entrepreneurs débutants ou des domaines d'activités commerciales rares, pour lesquels un comportement de paiement atypique est justifié par les particularités du domaine de l'activité en question.



Deuxièmement, l'ajustement constant du comportement des clients à haut risque par rapport au comportement normal habituel que nous avons constaté entraîne des changements constants des données analytiques elles-mêmes. Par conséquent, les modèles qui ont parfaitement fonctionné hier perdent très rapidement leur efficacité et doivent être remplacés par de nouveaux modèles. En même temps, plus nous surveillons ce domaine à l'aide d'outils d'apprentissage automatique et de modèles analytiques complexes, plus rapidement il change.

C'est pourquoi la mise en service d'outils d'intelligence artificielle dans le domaine de la surveillance financière est très différente de leur mise en œuvre dans d'autres domaines. Par exemple, dans le secteur du commerce en détail, le modèle de comportement universel des clients dans un magasin est assez précis et logique lorsqu'il est analysé à partir d'une grande quantité de données. Il est donc possible de prévoir avec succès le comportement des clients dans le magasin.

Après avoir expérimenté la difficulté de mettre en œuvre l'intelligence artificielle dans la surveillance financière, nous avons compris que nous étions compétents dans l'expertise des risques de BC/FT, mais que nous n'avions pas d'expertise interne dans l'application des outils d'apprentissage automatique, donc en 2022, nous avons décidé de commencer à embaucher des

analystes de données directement au sein de l'unité LBC/FT.

Il faut bien comprendre que l'analyste de données est tout à fait différent de l'analyste de clients que nous avons l'habitude de voir mener des enquêtes anti-blanchiment. Ils s'agit d'un employé tout à fait différent qui exige une communication personnalisée et des outils professionnels spéciaux. C'est ainsi que nos activités d'exploitation se sont enrichies de « bacs à sable », d'ordinateurs puissants, de moyens de programmation Python et d'outils de visualisation de données BI.

Ensuite, nous avons créé un réseau partenaire dans lequel les analystes clients ont été en mesure de formuler des hypothèses de recherche sur de nouvelles techniques possibles pour identifier les clients suspects, et les analystes de données ont réussi à numériser ces hypothèses dans des modèles appropriés. Les modèles reçus ont été mis en mode routine, et les résultats ont été renvoyés aux analystes clients pour vérification. Si l'efficacité des modèles diminuait, l'analyste clients formulait une hypothèse pour la préciser, ou une autre hypothèse dans le même domaine de risque, qui était transmise à l'analyste de données pour être mise en œuvre selon le cycle décrit ci-dessus.

La création d'un environnement de communication commun entre les analystes clients et les analystes de données a permis non seulement d'obtenir des effets synergiques dans

le cadre d'un travail commun, mais aussi d'améliorer les qualifications des employés et de développer de nouvelles compétences. Les analystes de données ont commencé à maîtriser leur domaine. Ils n'ont pas été chargés de se transformer en analystes clients, car de tels spécialistes travaillent déjà dans notre équipe. Mais ce rapprochement les a aidé à comprendre comment le domaine de la lutte contre le blanchiment d'argent est représenté spécifiquement en termes d'approches de traitement des données. En conséquence, les analystes de données ont commencé à sélectionner les outils de traitement de données les plus appropriés pour les différentes hypothèses.

Les analystes clients avançaient aussi. Si, auparavant, les questions liées aux technologies de l'information leur semblaient complexes et inaccessibles, c'est ensuite, après avoir vu comment tout fonctionne, qu'ils ont commencé à remplir certaines fonctions d'analyste de données. En outre, la familiarisation avec les outils d'analyse de données a permis aux analystes clients traditionnels de commencer à formuler des hypothèses d'identification des risques plus complexes.

En général, c'est une expérience assez intéressante que nous avons définie comme une collaboration entre l'intelligence naturelle et l'intelligence artificielle.

« APRÈS AVOIR EXPÉRIMENTÉ LA DIFFICULTÉ DE METTRE EN ŒUVRE L'INTELLIGENCE ARTIFICIELLE DANS LA SURVEILLANCE FINANCIÈRE, NOUS AVONS COMPRIS QUE NOUS ÉTIIONS COMPÉTENTS DANS L'EXPERTISE DES RISQUES DE BC/FT, MAIS QUE NOUS N'AVIONS PAS D'EXPERTISE INTERNE DANS L'APPLICATION DES OUTILS D'APPRENTISSAGE AUTOMATIQUE, DONC EN 2022, NOUS AVONS DÉCIDÉ DE COMMENCER À EMBAUCHER DES ANALYSTES DE DONNÉES DIRECTEMENT AU SEIN DE L'UNITÉ LBC/FT »



▲ Table ronde durant la finale de la IIIe Olympiade internationale sur la sécurité financière

Le cycle de fonctionnement décrit est utilisé de façon permanente, ce qui permet de :

1. Répondre rapidement aux nouveaux risques et typologies d'activités suspectes des clients dont la Banque de Russie et Rosfinmonitoring nous tiennent au courant. La mise en place de nouveaux modèles de risque ne prend pas plus de 2 jours ouvrables.
2. Toujours améliorer l'efficacité des règles analytiques appliquées pour la surveillance en ligne et hors ligne des opérations des clients. Par conséquent, nous pouvons nous permettre de ne pas augmenter le nombre d'employés alors que notre clientèle ne cesse de croître.
3. Tester nos propres hypothèses en quantité considérable pour identifier de nouveaux types et des variations actualisées d'anciens schémas de transactions suspectes. Chaque trimestre, au moins 10 hypothèses passent de

l'état d'idée à celui d'algorithme opérationnel.

Je vais vous faire part d'une autre observation intéressante. En octobre 2023, dans le cadre de Olympiade sur la sécurité financière organisées par Rosfinmonitoring, nous avons organisé un atelier pour les étudiants, au cours duquel nous avons parlé de notre projet analytique « Patterns ». Il s'agit d'un projet interne visant à développer un nouvel outil de haute performance pour identifier les transactions suspectes des clients.

En fait, l'opportunité même de nous impliquer dans ce projet est venue de notre expérience accumulée dans l'apprentissage automatique avec des analystes de données et de la compétence de formulation d'hypothèses analytiques acquise par les analystes clients.

Nous partageons donc cette impression de symbiose réussie avec les étudiants et imaginons qu'il serait merveilleux qu'à l'avenir ces

compétences puissent être incarnées par un seul employé qui analyse les clients, synthétise des hypothèses, les programme de manière autonome et les applique pour identifier les transactions à haut risque.

Le public nous demande pourquoi ce n'est pas actuellement le cas. Imaginez-vous que nos étudiants actuels qui participent à l'Olympiade sur la sécurité financière organisée par Rosfinmonitoring, ont envie de devenir de tels spécialistes dans le futur. Ils ne se contentent pas d'imaginer, ils se préparent toujours à ce type de travail, en accumulant des connaissances et en développant les compétences nécessaires.

Avec une telle jeune génération, nous avons un bel avenir devant nous dans le domaine de la surveillance anti-blanchiment. Un avenir dans lequel l'intelligence humaine et l'intelligence artificielle interagissent et évoluent d'une manière efficace.

ALEXEÏ GUELETA :

« LE MARCHÉ DE LA TECHNOLOGIE FINANCIÈRE DE RUSSIE EST UN DES PLUS INNOVANTS ET AVANCÉS DANS LE MONDE ENTIER »



Des expertises indépendantes sont organisées avant de mettre en œuvre les initiatives de la technologie financière. Les projets sont évalués en fonction des éventuels risques et menaces, ainsi que leurs avantages pour les citoyens, l'État et les entreprises. Cette expertise est organisée par le Groupe de conformité numérique du Centre d'analyse auprès du Gouvernement de la Fédération de Russie. Les journalistes de la revue ont interrogé Alexeï Gueleta, le directeur du Groupe à propos des fonctions de la division et de son rôle dans la culture financière d'aujourd'hui



1. Rosfinmonitoring (Service fédéral de surveillance financière) coopère dans divers domaines avec le Centre d'analyse auprès du Gouvernement de la Fédération de Russie. De plus, des projets ont été mis en œuvre avec le Groupe de conformité numérique que vous dirigez. Parlez-nous s'il vous plaît des objectifs du Groupe, et comment vous personnellement avez-vous abordé ce secteur.

En 2020, à l'initiative du Gouvernement de la Fédération de Russie, un nouveau domaine d'expertise pour le secteur public « la conformité numérique » a été créée sur la base du Centre d'analyse auprès du Gouvernement de la Fédération de Russie. Ses principales tâches consistent à coordonner le travail interministériel sur les initiatives de la technologie financière et à organiser une expertise d'analyse et de droit détaillée et indépendante, en prenant en compte l'expérience internationale. Nous travaillons dans les domaines liés à l'identification des risques et des menaces et au développement du marché des technologies financières, en prenant à la considération les besoins de l'État, des entreprises et des citoyens.

J'ai fait connaissance avec le fonctionnement du système de conformité quand j'étais étudiant. Je suis diplômé du Département spécialisé de l'Institut de sécurité financière et économique de UNRN IGPM (Université nationale de recherche nucléaire Institut de génie physique de Moscou), fondée avec le soutien de Rosfinmonitoring. Les professeurs étaient les fonctionnaires du Service, ce qui permet d'acquérir non seulement des connaissances théoriques, mais aussi des savoir-faire, y compris durant des stages effectués au sein de Rosfinmonitoring. J'ai acquis une expérience fondamentale et diversifiée en matière de conformité en travaillant dans le secteur bancaire. J'ai participé à la mise en place et à l'automatisation du système de gestion des risques réglementaires (conformité) au niveau du siège de la banque et à la coordination des établissements financiers russes et étrangers du groupe bancaire dans les domaines de LBC/FT et des risques réglementaires (conformité). Il fallait assurer le respect des normes uniformes du groupe bancaire, tout en tenant compte des particularités de la législation locale du pays en la matière.

2. Quels sont les domaines principaux en charge du Groupe de conformité numérique ?

On peut distinguer trois domaines principaux :

1. Les domaines qui se trouvent dans la zone « grise » et qui exigent une expertise complète et de recommandations pour la prise de décisions de gestion ultérieures, tant au niveau fédéral que régional. Il s'agit notamment de l'extraction et de la circulation des monnaies numériques. Nous devons nous immerger dans des projets spécifiques initiés par des représentants d'entreprises liés au développement de systèmes automatisés, de technologies blockchain et de systèmes de paiement.

2. Identification des risques et des menaces pour le système financier national et le secteur économico-social. On a travaillé sur l'identification des infractions liées à la détection des transactions bancaires illégales (miscoding), à la fraude sous couverture de prestations sociales et de cashback, aux ressources illégales lors de la pandémie du COVID-19 et bien d'autres. Nous n'allons pas entrer dans les détails du flux de travail et des résultats, mais nous avons besoin de bien comprendre les principales causes des menaces, d'élaborer des parcours client et des processus d'affaires, d'identifier les zones les plus vulnérables, de générer des flux de données, d'élaborer des tableaux de bord analytiques, de participer à des activités interministérielles et de préparer des rapports analytiques avec des recommandations visant à minimiser ou à éliminer les menaces identifiées.

3. Participation au développement des systèmes de paiement. Malgré la pression extérieure, le marché de la technologie financière de Russie est un des plus innovants et avancés dans le monde entier. Cependant, nous avons des choses

à améliorer et, par conséquent, il nous faut mettre à jour les approches conservatrices ou créer de nouvelles conditions de réglementation pour le développement du système financier. Dans la résolution de ces problèmes, il est important qu'existe une communication et une compréhension permanente entre les hommes d'affaires qui proposent de nouvelles idées pour le développement du système financier national et les autorités qui assurent la sécurité du système financier dans le cadre de leurs compétences.

Le Centre de coordination du Gouvernement de la Fédération de Russie facilite la compréhension entre les participants sans barrières bureaucratiques inutiles et l'avancé significative de progrès dans la résolution de problèmes actuels.

3. Quels sont les processus de la technologie financière que vous considérez comme conservateurs ?

Problèmes d'identification des citoyens, en particulier lors de l'ouverture d'un compte bancaire. Dans divers domaines sociaux et économiques, nous constatons une numérisation réussie des processus. Il est devenu plus pratique et plus rapide pour les gens de résoudre leurs problèmes quotidiens et professionnels par le biais de services à distance, ce qui n'est pas le cas pour l'ouverture d'un compte bancaire.

Néanmoins, nous avons réussi à avancer dans ce domaine. À la suite des demandes formulées par les représentants du secteur bancaire, le Centre de coordination en collaboration avec la Banque de Russie, Rosfinmonitoring et d'autres agences compétentes, a commencé à mettre au point des systèmes d'identification à distance des citoyens étrangers lors de l'ouverture d'un compte bancaire auprès d'un établissement de crédit russe. Ce projet est connu sous le nom de « Carte touristique ». Grâce au travail

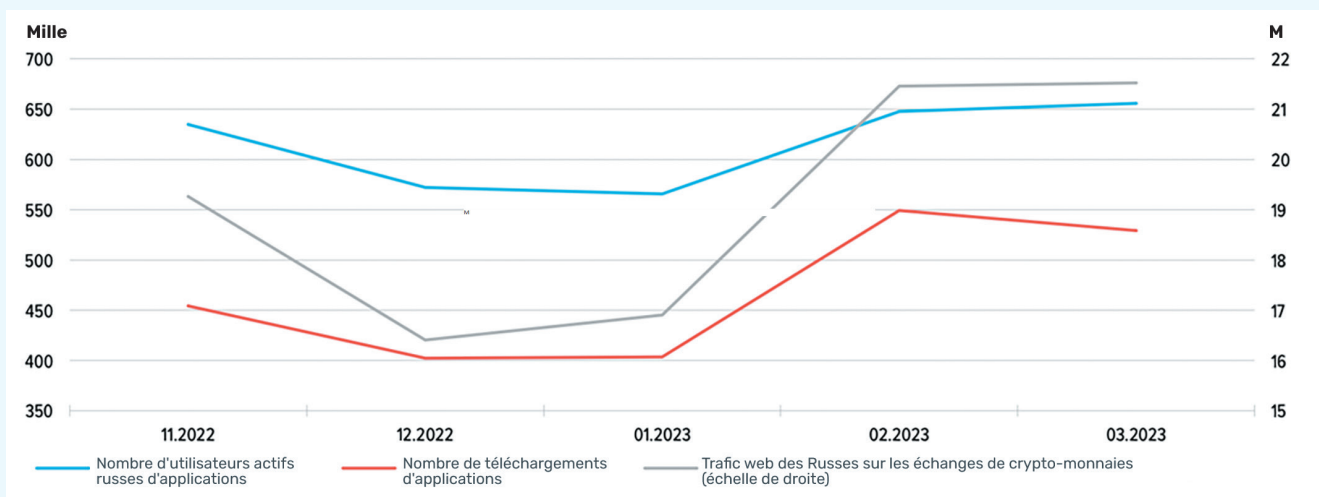
coordonné, on a réussi à modifier la législation nationale dans la lutte contre le blanchiment. Désormais, si certains critères et conditions sont remplis, les citoyens étrangers peuvent ouvrir un compte bancaire à distance auprès d'un établissement de crédit russe, obtenir une carte MIR virtuelle et commencer à dépenser de l'argent avant d'arriver en Russie. Cependant, les établissements de crédit nous font déjà part de difficultés qui surviennent et doivent être résolues ensemble.

La réglementation de l'extraction et de la circulation des crypto-monnaies est également un sujet brûlant depuis de nombreuses années. Toutes les agences sont conscientes que les crypto-monnaies comportent des risques et des menaces, mais il n'y a pas de consensus sur la manière de les gérer. En fait, il y a deux groupes : certains pensent que pour minimiser les risques et les menaces, il est nécessaire d'interdire la circulation des crypto-monnaies impliquant le système financier russe, tandis que d'autres pensent qu'il faut créer des conditions réglementaires claires pour tous les acteurs du marché russe des crypto-monnaies. En tant qu'expert, et compte tenu de l'intérêt croissant* des citoyens pour ce produit numérique, je suis plutôt pour adopter une approche fondée sur les risques pour réglementer le marché des crypto-monnaies, qui séparera les acteurs fiables et les malhonnêtes. En effet, tout interdire est la solution la plus facile, mais la manière dont les autorités et les établissements de crédit peuvent garantir le respect effectif de l'interdiction à l'avenir est une bonne question, qui peut provoquer des amendes pour les établissements de crédit et des dispositions légales « inapplicables ».

4. Qu'en pensez-vous, les nouvelles technologies, peuvent-elles renforcer la protection des utilisateurs de services financiers contre les fraudeurs ? Ou, au contraire, s'agit-il plutôt d'un



► Activité des utilisateurs russes sur les échanges de crypto



Source : https://www.cbr.ru/Collection/Collection/File/44007/4q_2022_1q_2023.pdf

instrument supplémentaire pour les criminels ?

Et c'est là que réside le paradoxe : les nouvelles technologies peuvent à la fois renforcer la sécurité et devenir un instrument supplémentaire pour les criminels. L'expérience montre que les fraudeurs commencent à utiliser les nouvelles technologies bien avant que les autorités n'y prêtent attention. Pour ne pas affirmer sans preuves, vous pouvez au moins faire connaissance avec des fraudes à l'aide de la technologie Deepfake et les arnaques par usurpation de voix. Il y a une tendance négative et cela ne fera que se développer.

5. Le Centre d'analyse a-t-il mené des études spécifiques sur le rôle de la culture financière dans le contexte de la numérisation ? Quels projets dans ce domaine vous semblent prometteurs ?

Les statistiques actuelles sont décevantes : d'une année à l'autre, les pertes des citoyens dues aux fraudes utilisant les services numériques augmentent. Selon la Banque de Russie, en 2023 les cybercriminels ont volé 15,8 milliards de roubles aux russes. Ceci ressort de l'Évaluation des transactions effectuées sans le consentement préalable des clients des établissements financiers. En 2023, les transactions¹ sans le

consentement préalable des clients ont augmenté de 11,48 % par rapport à 2022.

En Russie, diverses agences ont constitué une vaste base de connaissances pour améliorer la culture financière. En particulier, Rosfinmonitoring organise avec succès une Olympiade internationale sur la sécurité financière et a acquis une expérience considérable des cas pratiques qui seront utiles aux citoyens dans le contexte d'une numérisation intensive. La formation peut être réalisée sous la forme de jeux en ligne, du quiz et autres formats numériques dont la mise en œuvre peut être recommandée dans les établissements d'enseignement, les organismes publics, les entreprises et d'autres institutions.

6. Conformité numérique en Russie : y a-t-il des caractéristiques uniques ?

Si vous posez une question sur la fonction de conformité numérique dans les établissements de crédit russes, personne ne peut mieux vous renseigner que les services de conformité de ces banques. On peut envisager la discussion de ce problème au sein du Conseil de conformité organisé par Rosfinmonitoring. J'y participerais avec plaisir.

En ce qui concerne l'unité dont je suis responsable, les caractéristiques particulières suivantes peuvent être notées : le Groupe de conformité numérique fonctionne sur la plateforme du Centre de coordination auprès du Gouvernement de la Fédération de Russie et c'est un hub d'experts indépendants pour le Gouvernement de la Fédération de Russie qui sont sollicités lorsqu'il s'agit d'une prise des décisions de gestion.

► **« LA RÉGLEMENTATION DE L'EXTRACTION ET DE LA CIRCULATION DES CRYPTO-MONNAIES EST ÉGALEMENT UN SUJET BRÛLANT DEPUIS DE NOMBREUSES ANNÉES. TOUTES LES AGENCES SONT CONSCIENTES QUE LES CRYPTO-MONNAIES COMPORTENT DES RISQUES ET DES MENACES, MAIS IL N'A PAS DE CONSENSUS SUR LA MANIÈRE DE LES GÉRER »**

¹ <https://www.cbr.ru/press/event/?id=18419>



DÉTECTION ET LUTTE CONTRE LA CYBERCRIMINALITÉ

50 BOGDAN CHABLYA

La lutte contre les « mules financières » et les opérations P2P à haut risque est une priorité de la surveillance financière

53 VADIM OUVAROV

Sécurité de l'information du marché financier : question de la lutte contre la cyberfraude dans les transferts de fonds

57 ANTON RASTACHTENOV

Restriction préalable de l'accès à des informations sur Internet dont la diffusion est interdite sur le territoire de la Fédération de Russie

60 ROMAN MOUKHLYNOV

Les dernières tendances sur le marché des fournisseurs illégaux de services financiers

63 OLEG KIPKAÏEV

L'utilisation des technologies numériques dans la collecte, le traitement et la généralisation des données informatiques et analytique ainsi que d'autres données utilisées dans les activités du parquet, par exemple dans le cadre des fonctionnalités du système d'information et d'analyse « Bureau électronique du procureur »

LA LUTTE CONTRE LES «MULES FINANCIÈRES» ET LES OPÉRATIONS P2P À HAUT RISQUE EST UNE PRIORITÉ DE LA SURVEILLANCE FINANCIÈRE



 **BOGDAN CHABLYA,**
Directeur du Département de
surveillance financière et de contrôle
des changes de la Banque de Russie

La Banque de Russie note les risques accrus de l'utilisation du secteur bancaire russe pour les transactions P2P par des particuliers pour les règlements entre les citoyens et l'économie souterraine. Ces risques sont directement liés au service rendus par les banques aux prête-noms ce qui on appelle « mules financières », sur les comptes desquels les transactions P2P sont effectuées. La Banque de Russie, en pleine collaboration avec les banques, développe et met en œuvre des approches pour contrer de telles opérations, y compris des mesures visant à améliorer la vitesse de détections des comptes des personnes physiques « mules financières », ainsi que la riposte aux risques identifiés

Le contrôle et la surveillance des opérations des établissements de crédit indique l'utilisation par des acteurs malhonnêtes des services P2P des établissements de crédit pour effectuer des opérations à haut risque. Ces transactions permettent aux entreprises souterraines pour lesquelles l'accès aux services bancaires légaux est interdit d'obtenir de l'argent. Le secteur parallèle comprennent les casinos en ligne et les bookmakers, les pyramides financières, les vendeurs du contenu piraté, divers types de

sites web frauduleux, les vendeurs de biens interdits, les bureaux d'échange de crypto-monnaies et les services P2P de bourses de crypto-monnaies qui utilisent des comptes de « mules financières ».

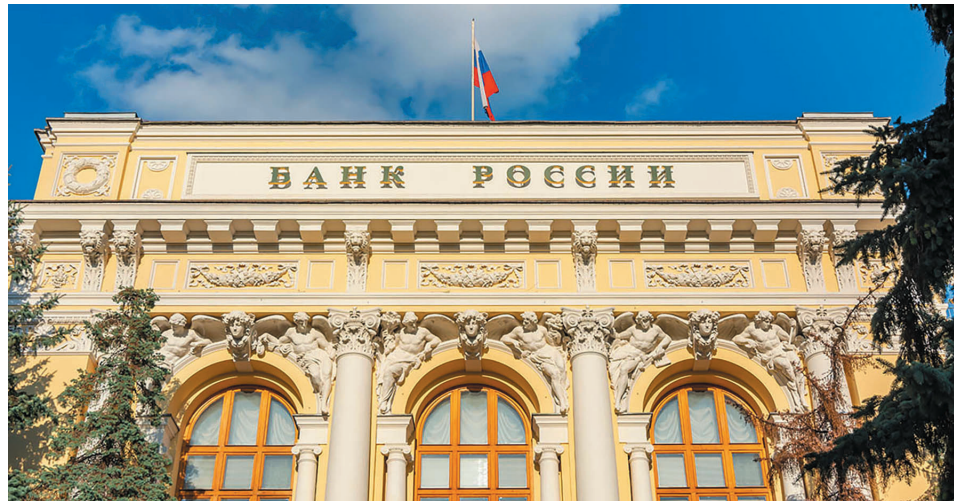
Nous prenons comme point de départ que l'implication des citoyens dans de telles opérations comporte des risques non seulement de perdre leur épargne suite aux divers types de fraudes, mais aussi des risques d'implication dans des activités illégales, ce qui peut entraîner une

responsabilité pénale. Cependant, si les banques mènent de telles opérations, compte tenu du volume élevé de transactions dans ce secteur parallèle, cela peut constituer une menace pour les intérêts des créanciers et des déposants.

En 2020-2022, ces transactions ont été réalisées en utilisant les services d'acquiring du secteur bancaire et se sont concentrées principalement dans les petits établissements de crédit spécialisés dans la prestation de services bancaires parallèles.

En règle générale, les règlements ont été effectués via de comptes de prestataires de services de paiement étrangers, de personnes morales et d'entrepreneurs individuels créés pour ce type d'opérations, d'établissement financiers frauduleux menant des activités illégales sous couvert de mini prêts, par exemple.

Pendant cette période, la Banque de Russie a éliminé du système du secteur bancaire les opérations à haut risque et des établissements financiers qui les fournissent.



LE LANCEMENT DE LA PLATEFORME « CONNAÎTRE SON CLIENT »

a rendu beaucoup plus difficile l'utilisation de comptes de personnes morales et d'entrepreneurs individuels pour ce type de transactions. L'arrêt des activités de systèmes de paiement internationaux qui effectuaient auparavant des transactions à haut risque via de banques acquéreuses étrangères, a également changé d'une manière significative le marché des paiements parallèles.

Par conséquent, en 2023, nous observons une évolution du volume des transactions à haut risque vers des règlements P2P directs via des cartes de paiement et des « mules financières » qui ouvrent un compte ou une carte bancaire à leur nom auprès d'une banque pour les transmettre ensuite à la disposition des acteurs du secteur parallèle. En ce qui concerne les transactions P2P, on peut donner un exemple des transactions « carte à carte », « portefeuille à portefeuille », « du compte d'abonné d'un opérateur mobile à un portefeuille ou à une carte et vice-versa ».

En ce moment, nous évaluons le volume des transactions P2P à haut risque dans le secteur bancaire,

ainsi que le nombre de « mules financières » impliquées dans ses opérations, comme élevé, et cela exige une réponse globale de notre part. La direction de la Banque de Russie considère que ce type de travail est prioritaire.

D'une part, selon nos estimations, pour le secteur parallèle l'utilisation de systèmes de paiement P2P avec les citoyens est plus difficile et plus cher que les opérations d'acquisition, y compris en raison de la nécessité de maintenir l'infrastructure de la composante informatique chargée de l'automatisation des opérations et de l'enregistrement des transactions, et de nombreux comptes de prête-noms - « mules financières ». D'autre part, plusieurs facteurs ont contribué à la réorientation des participants au secteur parallèle vers l'utilisation de ce schéma :

- la simplicité et la disponibilité des cartes bancaires et des portefeuilles électroniques qui permettent d'effectuer plusieurs transactions P2P, pratiquement sans restrictions et avec des commissions minimales. D'un côté, cela rend ces produits bancaires pratiques pour la population et les entreprises. D'un autre côté, la facilité d'ouverture et la disponibilité des produits bancaires sont

utilisées par les acteurs du secteur bancaire parallèle. Par exemple, par les soi-disant « chefs des mules financières » qui ouvrent des comptes pour une telle entreprise. Ils s'adressent à des citoyens moins renseignés qui sans connaître toutes les conséquences, transfèrent le compte qu'ils viennent d'ouvrir (portefeuille) à la gestion des tiers. Des dizaines de cartes virtuelles sont enregistrées au compte, via lesquelles des sommes importantes sont transférées en quelques jours.

- la possibilité d'identifier les personnes physiques lors de l'ouverture de portefeuilles électroniques avec l'implication d'entreprises extérieures (par exemple, des agents payeurs bancaires, des opérateurs mobile) qui peuvent souvent adopter une approche formelle pour satisfaire aux exigences d'identification, puisque le montant des revenus qu'elles reçoivent dépend du nombre de portefeuilles électroniques qu'elles ouvrent pour les personnes physiques. Lors de l'identification (identification simplifiée) la législation en vigueur autorise de confirmer l'authenticité des informations soumises en utilisant les systèmes

d'information d'État sans présence physique et fourniture de documents originaux pour ouvrir des portefeuilles électroniques. Nous avons identifié des cas où des établissements de crédit ont ouvert des portefeuilles électroniques en utilisant les données personnelles des personnes sans qu'ils le sachent et en effectuant des transactions sur ces portefeuilles, ce qui a créé des risques importants pour ces personnes.

- certains services P2P d'établissements de crédit accessibles au public sur Internet sont vulnérables du point de vue technique. Les organisateurs du secteur parallèle utilisent des formes de paiement fictifs P2P sur leurs sites web où les « robots » recueillent les données des cartes bancaires des citoyens et les redirigent automatiquement vers la page Internet réelle de l'établissement de crédit pour effectuer des transactions P2P.

Afin de prévenir ces risques, la Banque de Russie a publié les recommandations méthodologiques n° 16-MP¹ du 06/09/2021 et n° 13-MP² du 12/10/2023.

Selon les recommandations méthodologiques n° 16-MP les établissements de crédit doivent identifier les transactions impliquant le virement de fonds (monnaie électronique) entre les personnes physiques à l'aide de moyens de paiement électroniques (en particulier les cartes de paiement et les portefeuilles électroniques) qui se diffèrent des règlements ordinaires et appliquer des mesures anti-légalisation, ainsi qu'assurer la

protection de l'information nécessaire de leurs propres services P2P contre une utilisation par des robots.

Afin de réduire les risques liés à l'utilisation des services d'acquisition en contournant les recommandations méthodologiques n° 16-MP, la Banque de Russie a publié les recommandations méthodologiques n° 13-MP, dans lesquelles il est notamment recommandé aux établissements de crédit-acquéreurs de contrôler l'arrivée des fonds sur les comptes de l'entreprise de commerce et de services où l'achat a été effectué (ce qui met fin à ce que l'on appelle le « schéma du restaurant »), ainsi que de faire attention aux signes de virements non habituels en faveur d'entreprise de commerce et de services qui n'exercent pas d'activité économique réelle.

Nous travaillons actuellement en coopération étroite avec les banques pour développer et mettre en œuvre de nouveaux outils modernes pour contrer les transactions P2P à haut risque, qui comprennent également des procédures de contrôle supplémentaires pour

l'enregistrement des cartes bancaires et l'utilisation de certains produits bancaires ainsi qu'une détection plus rapide, y compris en ligne, des comptes et des transactions des personnes physiques (« mules financières »).

Ce travail vise tout d'abord à rendre plus difficile le fonctionnement du secteur parallèle comme l'utilisation du secteur bancaire et des opérations P2P soit aussi peu pratique et coûteuse que possible.

Deuxièmement, il s'agit d'inculquer aux établissements financiers et au public une tolérance zéro à l'égard des activités des « mules financières ». Cela devrait être favorisé par l'élaboration de procédures de conformité par le secteur bancaire afin d'empêcher la possibilité de gérer des comptes de prête-noms, et par la sensibilisation menée par la Banque de Russie et les établissements de crédit en collaboration avec les forces de l'ordre afin d'informer les citoyens des conséquences de ces activités et de provoquer une attitude négative à leur égard.

➤ NOUS TRAVAILLONS ACTUELLEMENT EN COOPÉRATION ÉTROITE AVEC LES BANQUES POUR DÉVELOPPER ET METTRE EN ŒUVRE DE NOUVEAUX OUTILS MODERNES POUR CONTRER LES TRANSACTIONS P2P À HAUT RISQUE, QUI COMPRENNENT ÉGALEMENT DES PROCÉDURES DE CONTRÔLE SUPPLÉMENTAIRES POUR L'ENREGISTREMENT DES CARTES BANCAIRES ET L'UTILISATION DE CERTAINS PRODUITS BANCAIRES AINSI QU'UNE DÉTECTION PLUS RAPIDE, Y COMPRIS EN LIGNE, DES COMPTES ET DES TRANSACTIONS DES PERSONNES PHYSIQUES (« MULES FINANCIÈRES »)

¹ Sur l'attention accrue des établissements de crédit à l'égard de certaines transactions des personnes physiques.

² Concernant les activités des établissements de crédit et des agrégateurs de paiement pour les règlements avec les fournisseurs de biens (services) pour les transactions effectuées à l'aide de moyens de paiement électroniques.

SÉCURITÉ DE L'INFORMATION DU MARCHÉ FINANCIER: QUESTION DE LA LUTTE CONTRE LA CYBERFRAUDE DANS LES TRANSFERTS DE FONDS



VADIM OUVAROV,
Directeur du Département de la
sécurité de l'information de la
Banque de Russie

L'omniprésence et l'utilisation des technologies de paiements numériques ont fondamentalement changé l'attitude de la société à l'égard du problème de la sécurité de l'information. Avec le développement rapide des services bancaires à distance, l'absence de mesures appropriées pour protéger les clients des banques contre les cyberfraudeurs peut avoir des effets négatifs pour la société¹. Par conséquent, aujourd'hui, la capacité à faire face aux risques de détournement de fonds des comptes des citoyens est l'un des facteurs clés de la protection des droits des consommateurs de services financiers et de l'augmentation de la confiance aux technologies numériques

La lutte contre la cyberfraude dans le secteur financier est l'une des priorités de la Banque de Russie. D'après les résultats des travaux systématiques menés par le régulateur en coopération avec les représentants du secteur, les banques ont repoussé près de 34,8 millions de tentatives de

transactions frauduleuses en 2023. Cela a permis d'éviter le détournement de 5,8 milliards de roubles des clients d'établissements de crédit.

En même temps, au cours des dernières années, la Banque de Russie a enregistré une augmentation annuelle du volume des transactions

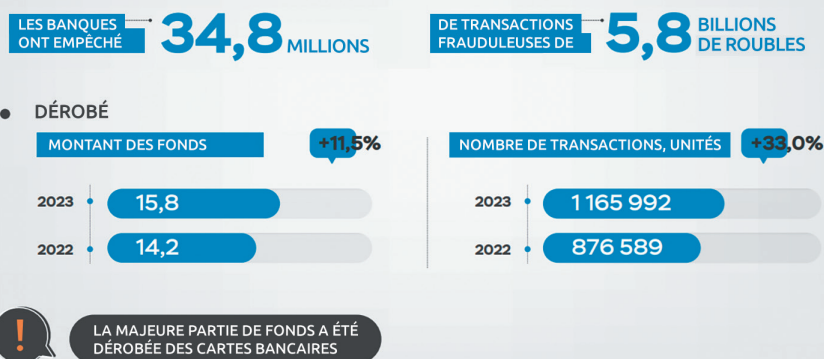
réussies effectuées sans le consentement préalable des clients de la banque. En 2023, les malfaiteurs ont volé 15,8 milliards de roubles. Par rapport à l'année précédente, le montant d'argent volé a augmenté de 11,5 %. Le nombre de transactions frauduleuses a augmenté de 33% et a dépassé 1,1 million².

¹ Conformément aux données officielles du ministère russe de l'Intérieur, en 2023, un crime sur trois dans notre pays a été commis à l'aide des technologies de l'information et des télécommunications. Dans ce domaine, on constate une augmentation de 29,7% d'infractions pénales qu'en 2022 (<https://mydmedia.ru/news/official/statisticheskie-svedeniya-o-sostoyanii-prestupnosti-v-2023-godu/>).

² Les évaluations annuelles des transactions effectuées sans le consentement préalable des clients des établissements financiers sont publiés sur le site officiel de la Banque de Russie (http://www.cbr.ru/analytics/ib/operations_survey/2023/).



TRANSACTIONS FRAUDULEUSES : STATISTIQUES



L'un des facteurs qui empêchent un changement radical de la situation en matière de lutte contre la fraude et l'ingénierie sociale est l'amélioration constante des schémas et des scénarios d'influence des malfaiteurs sur les citoyens.

Actuellement, il existe une tendance à des attaques personnalisées dont l'exécution est précédée d'une étude détaillée des informations personnelles des victimes potentielles, y compris les informations publiées par les citoyens sur différentes ressources sur Internet.



La Banque de Russie prend des mesures exhaustives pour lutter contre l'hameçonnage par téléphone et les arnaques sur Internet. L'ensemble des mesures prises comprend l'amélioration de la législation régissant les activités des établissements financiers, la sensibilisation des citoyens, ainsi qu'une interaction avec les forces de l'ordre, les organismes de surveillance, les enregistreurs de noms de domaine et les opérateurs mobile.

En juillet 2024, la loi sur l'amélioration des pratiques de la lutte contre le détournement de fonds des clients des banques, élaborée avec

la participation de la Banque de Russie, entrera en vigueur³. La loi prévoit :

- l'introduction d'une « période de réflexion » de deux jours. C'est une procédure obligatoire pour qu'une banque suspende les transferts de fonds utilisant des détails dont les informations sont contenues dans la base de données de la Banque de Russie « Sur les cas et les tentatives de transfert de fonds sans le consentement préalable du client » (ci-après dénommée la base de données de la Banque de Russie). En deux jours, la personne sera capable de réfléchir et d'évaluer les actions entreprises et de refuser

d'effectuer un virement sur un compte suspect ;

- l'obligation de la banque de désactiver l'accès aux moyens de paiement électroniques des « mules financières » si la base de données de la Banque de Russie a reçu des informations de la part du Ministère de l'Intérieur de Russie sur des actes illégaux commis par ces « mules ». En revanche, si la base de données de la Banque de Russie a reçu l'information d'un établissement financier, la banque aura le droit de désactiver les moyens de paiement électroniques du client ;
- l'obligation de la banque de rembourser le client dans un délai de 30 jours si la banque a autorisé le transfert de fonds vers un compte frauduleux figurant dans la base de données de la Banque de Russie sans prendre les mesures indispensables pour protéger le client.

Les résultats d'un sondage mené par la Banque de Russie en 2023 sur le niveau de satisfaction à l'égard de la sécurité des services financiers ont montré que près de 62 % des citoyens victimes de fraudeurs



PORTAIT D'UNE VICTIME

UNE FEMME QUI TRAVAILLE
TOUCHE UN SALAIRE
MOUYEN BACHELIÈRE

RÉSIDE EN VILLE

LE MONTANT DÉROBÉ
EST MOINS DE 20 MILLE
ROUBLES

ÂGÉE DE 25 À 44 ANS



ENVIRON UN TIERS DES VICTIMES DE FRAUDES PORTENT UNE PLAINTÉ AUPRÈS DE LEUR BANQUE

³ Loi fédérale n° 369-FZ du 24 juillet 2023 « Sur la modification de la Loi fédérale » Sur le système de paiement national ».

L'APPEL TÉLÉPHONIQUE EST L'OUTIL PRINCIPAL DES MALFAITEURS

LES NUMÉROS QUE LES FRAUDEURS UTILISENT POUR LES APPELS



LES MALFAITEURS PRÉFÈRENT PLUTÔT LES MESSAGERIES INSTANTANÉES POUR TROMPER LES GENS

ont présenté une demande auprès de la banque et/ou se sont adressés à la police. Le développement de l'échange d'informations sur les transactions frauduleuses entre les banques et les forces de l'ordre est très important.

En octobre 2023, la loi sur l'échange d'informations de la Banque de Russie et le Ministère de l'Intérieur de Russie est entrée en vigueur⁴. Cette loi a créé les conditions d'un échange automatisé de données sur les transactions sans le consentement préalable des clients entre les institutions gouvernementales. Désormais, les forces de l'ordre peuvent obtenir le plus vite possible les informations nécessaires aux enquêtes sur les fraudes et aux affaires pénales à partir de la base de données de la Banque de Russie. Les informations que la Banque de Russie reçoit du Ministère de

l'Intérieur de Russie peuvent être prises en compte par les banques dans leurs systèmes anti-fraude afin de prévenir de nouvelles transactions frauduleuses.

Afin de lutter contre les actions illégales sur Internet, la banque de Russie coopère avec le Parquet général de la Fédération de Russie⁵ et les bureaux d'enregistrement de noms de domaine. En 2023, le régulateur leur a envoyé plus de 38,3 mille de ressources Internet utilisées pour mener des activités illicites afin de les bloquer. La majeure partie de ces ressources (55 %) sont des sites d'hameçonnage, dont l'objectif principal est de voler les données des clients des établissements financiers. En outre, la restriction de l'accès à 4,5 mille pages (groupes) dans les réseaux sociaux et à 35 applications qui ont été principalement utilisées par des

malfructeurs pour mener des activités non autorisées et l'hameçonnage sous le couvert d'établissements de crédit existants.

La Banque de Russie a envoyé 575 700 numéros de téléphone aux opérateurs mobile afin de bloquer ceux utilisés par les fraudeurs pour voler l'argent des citoyens.

Compte tenu des résultats de la surveillance effectuée par la Banque de Russie cette année, l'attention du régulateur se concentre sur deux tendances qui ont des conséquences sociales négatives pour les citoyens : un volume important de fraudes aux crédits et l'implication de citoyens, en particulier des jeunes, dans les « mules financières ».

Le problème de la fraude au crédit est dangereux non seulement parce que le montant moyen détourné

⁴ Conformément à la Loi fédérale n° 408-FZ du 20 octobre 2022 « Sur les modifications de l'Article 26 de la Loi fédérale » Sur les banques et les activités bancaires et de l'Article 27 de la Loi fédérale « Sur le système national de paiement ».

⁵ Dans le cadre des pouvoirs prévus par l'Article 6.2 de la loi fédérale n° 86-FZ du 10/07/2002 « Sur la Banque centrale de la Fédération de Russie (Banque de Russie) ».

augmente. Les citoyens qui, sous l'influence de malfaiteurs obtiennent un prêt et leur transfèrent les fonds empruntés, se trouvent dans une situation « l'abîme de dette » pendant de nombreuses années. Afin de protéger les citoyens et d'augmenter la responsabilité des établissements de crédit, la Banque de Russie étudie les initiatives pertinentes. Celles-ci incluent le « délai de réflexion » entre l'approbation du prêt et le transfert de fonds à l'emprunteur : tout d'abord, cette mesure devrait concerner les cas où l'emprunteur obtient un prêt pour un montant considérable. Il est également important d'intégrer des procédures anti-fraude dans le processus d'octroi des prêts afin de s'assurer que lorsqu'une banque donne des fonds, elle sait si une personne est sous l'influence de tiers ou non.

La Banque de Russie lutte également activement contre les « mules financières », activité qui consiste à retirer et à encaisser de fonds qui constituent un produit du crime, y compris par l'utilisation de moyens de paiement électroniques par des citoyens impliqués dans ce type d'activité. Il existe différentes façons de se trouver impliqué dans les « mules financières ». Dans certains cas, les personnes s'engagent dans ces activités consciemment, mais parfois sans en réaliser des conséquences. Dans d'autres cas, ils n'ont pas conscience d'être impliqués dans des activités illégales en partageant leurs données personnelles avec quelqu'un, en les publiant dans le domaine public, par exemple sur les réseaux sociaux, ils peuvent devenir complices d'un crime. Les groupes d'âge les plus vulnérables sont les adolescents et les jeunes (l'âge principal des « mules financière » est de 17 à 19 ans).

Pour résoudre ce problème, en avril 2022 la Banque de Russie a formulé des recommandations aux établissements de crédit sur la désactivation des moyens de paiement électroniques des personnes dont les cartes de paiement sont utilisées pour retirer et encaisser les fonds volés⁶. C'est pourquoi les banques ont déjà le droit de suspendre temporairement l'accès en ligne à la gestion des comptes lorsqu'un client effectue des transactions suspectes.

Lorsque la loi susmentionnée sur l'amélioration de la lutte contre le détournement de fonds des clients des banques entrera en vigueur en juillet 2024, les exigences relatives à la restriction de la banque à distance aux « mules financières » deviendront plus strictes. Les banques seront obligées de retenir le moyen de paiement électronique utilisé par le client si des informations sur des actes illégaux commis par celui-ci ont été envoyés à la base de données de la Banque de Russie par le Ministère de l'Intérieur de Russie. Cette information étant transmise à tous les établissements de crédit, les transactions à distance sur les comptes de « mules financières » seront suspendues dans toutes les banques.

Cette mesure contribuera à créer les conditions nécessaires pour que ce genre d'activités illégales soit économiquement défavorable pour les malfaiteurs.

Pour intensifier la sensibilisation des clients par les établissements de crédit, la banque de Russie a préparé et convenu avec le Ministère de l'Intérieur de Russie des Recommandations méthodologiques appropriées⁷. Elles comprennent

des mesures concrètes visant à sensibiliser les clients afin de lutter contre l'implication dans des « mules financières ». Les principaux objectifs de la sensibilisation sont d'informer sur la responsabilité et les conséquences de la participation à des activités de « mules financières », de faire savoir aux citoyens leur caractère illégal et la mauvaise réputation des activités de « mules financières ».

Le concept de lutte du secteur bancaire contre les diverses manifestations de la cyberfraude, y compris la fraude au crédit et les comptes des « mules financières », est en grande partie basé sur des données de haute qualité concernant les transactions suspectes que les banques envoient à la base de données de la Banque de Russie, et que le régulateur diffuse à son tour à tous les participants à l'échange d'informations. L'intégrité, la fiabilité et la ponctualité de ces informations dépendent de la rapidité et de l'efficacité de la lutte contre les malfaiteurs, ainsi que de la qualité des systèmes de lutte contre la fraude dans les banques. Par conséquent, l'une des principales priorités des activités d'organisme de réglementation, y compris des activités de surveillance, est de veiller à ce que les données soient correctement communiquées à la Banque de Russie aujourd'hui. Ceci est primordial pour garantir que les mécanismes de lutte contre le détournement de fonds prévus par les lois adoptées protègent les droits et les intérêts des citoyens, consommateurs de services financiers.

⁶ Lettre d'information de la Banque de Russie n° 01-56-5/3143 du 15/04/2022 sur la mise en œuvre par les établissements de crédit des mesures visant à contrer la mise en œuvre des transferts de fonds sans le consentement préalable des clients.

⁷ Recommandations méthodologiques n° 3-MP du 28/02/2024 sur le renforcement de la sensibilisation des établissements de crédit auprès de leurs clients afin d'empêcher le transfert de fonds sans le consentement préalable du client, ainsi que la conclusion de contrats de crédit (prêt) sous l'influence de la tromperie ou de l'abus de confiance et l'exécution de transactions à l'aide de ces fonds, ainsi que l'implication de citoyens dans le retrait et l'encaissement de fonds obtenus par la voie criminelle.

RESTRICTION PRÉALABLE DE L'ACCÈS À DES INFORMATIONS SUR INTERNET DONT LA DIFFUSION EST INTERDITE SUR LE TERRITOIRE DE LA FÉDÉRATION DE RUSSIE

Ces dernières années, le problème des crimes commis avec des technologies de l'information et de la communication reste l'un des plus urgents et constitue une menace sérieuse pour la sécurité nationale de la Fédération de Russie



➤ ANTON RASTACHTCHENOV,
Chef du Département de la prévention de la diffusion et de la détection des informations destructives et interdites sur Internet Direction d'organisation de la lutte contre l'utilisation illégale des technologies de l'information et de la communication du Ministère de l'Intérieur de la Fédération de Russie Lieutenant-colonel de la police

Cela est dû à l'introduction accélérée de la technologie de l'information dans la vie quotidienne de la société, ce qui permet aux criminels de rester à l'abri des regards des forces de l'ordre.

Selon les statistiques officielles, de janvier à décembre 2023, les organes du Ministère de l'Intérieur ont enregistré 677 000 infractions commises à l'aide des technologies de l'information et de la communication, ce qui représente une augmentation de 29,7 % par rapport à l'année précédente.

L'augmentation constante du nombre d'infractions dans cette catégorie indique la nécessité de trouver les formes, les techniques et les moyens les plus adaptés et les plus efficaces pour les détecter, les prévenir, les réprimer, les résoudre et enquêter.

Dans l'ensemble des mesures d'enquête tendant à neutraliser les cybercrimes, les mesures préventives jouent un rôle important visant à contrer les ressources d'information illégales utilisées par les criminels à la fois comme plateformes de

publicité et de propagande et comme plateformes conçues pour blanchir les produits du crime et financer la criminalité.

Conformément à la législation en vigueur, le Ministère de l'Intérieur de Russie, en collaboration avec Roskomnadzor (Service fédéral de surveillance en matière des communications, technologies de l'information et médias), met en œuvre la fonction de restriction de l'accès aux ressources Internet contenant des informations interdites, des informations sur les drogues et les armes, ainsi que des informations à caractère extrémiste.

En 2023, grâce aux efforts concertés de ces agences, l'accès à plus de 330 000 sites web et pages comportant ce type de contenu a été restreint.

Les relations dans l'exercice du droit à la recherche, la réception, le transfert, la production et la diffusion de l'information, l'application des technologies de l'information, ainsi que la sécurité de l'information, sont régies par la Loi fédérale n° 149-FZ du 27 juillet 2006¹.

¹ La loi fédérale n° 149-FZ du 27 juillet 2006 « Sur l'information, les technologies de l'information et la sécurité d'information ». Ci-après la Loi fédérale n° 149-FZ.

En règle générale, les sources de diffusion d'informations interdites sont des ressources spéciales sur Internet, ce sont des sites web spécialisés et des pages de forums, ainsi que des groupes thématiques dans les réseaux sociaux. Dans le même temps, les personnes impliquées dans la création des plateformes susmentionnées peuvent se trouver à l'étranger et utiliser des instruments et des ressources pour modérer leur travail.

L'Article 15.1 de la Loi fédérale n° 149-FZ, entrée en vigueur le 1er novembre 2012, prévoit le blocage des ressources Internet, qui s'entend comme un ensemble de mesures organisationnelles et techniques visant à restreindre l'accès à des informations interdites diffusées sur Internet.

L'alinéa 2 de l'Article 15.1 de la Loi fédérale n° 149-FZ dispose que le système d'information automatisé unifié « Registre unifié des noms de domaine, des références aux pages web et des adresses de réseau permettant d'identifier les pages web contenant des informations dont la diffusion est interdite dans la Fédération de Russie »² comprend les noms de domaine et (ou) références aux pages web, ainsi que les adresses de réseau permettant d'identifier les sites Internet contenant des informations dont la diffusion est interdite dans la Fédération de Russie.

Conformément à l'alinéa 5 de l'Article 15.1 de la Loi fédérale n° 149-FZ, les motifs pour inclusion de ces ressources Internet dans le Système d'information automatisé unifié (SIAU) « Registre unifié » sont des décisions des autorités exécutives fédérales autorisées par le Gouvernement de la Fédération de Russie, adoptées dans le cadre de leurs compétences conformément à la procédure établie par le Gouvernement de la Fédération de Russie³, ainsi qu'une décision du tribunal déclarant que les informations diffusées sur l'Internet sont interdites dans la Fédération de Russie.

Sous-paragraphes « a-m » du paragraphe 1 de l'alinéa 5 de l'Article 15.1 de la Loi fédérale n° 149-FZ établit une liste exhaustive des informations interdites à l'égard desquelles les autorités exécutives fédérales autorisées par le Gouvernement de la Fédération de Russie prennent les décisions appropriées selon leurs compétences.

En particulier, les sous-paragraphes « b » et « k » du paragraphe 1 de l'alinéa 5 de l'Article 15.1 de la Loi fédérale n° 149-FZ définissent le motif d'inclusion dans le SIAU « Registre unifié » des ressources Internet qui diffusent des informations :

- sur les moyens, les méthodes de développement, de fabrication et d'utilisation des stupéfiants, des substances psychotropes et de leurs précurseurs, les lieux d'achat de ces stupéfiants, substances et précurseurs, les moyens et lieux de culture des plantes psychotropes ;

- techniques, méthodes de fabrication improvisée d'explosifs et d'engins explosifs, fabrication ou conversion illégale des armes, de pièces principales d'armes à feu, ainsi que fabrication illégale de munitions, à l'exception des informations sur les méthodes, techniques de munitions indépendantes pour les armes à feu civiles à canon long.

La stratégie de la sécurité nationale de la Fédération de Russie, approuvée par le Décret n° 683 du 31 décembre 2015 du Président de la Fédération de Russie, classe les activités liées à l'utilisation des technologies de l'information et de la communication pour la diffusion et la propagande de l'idéologie fasciste, de l'extrémisme, du terrorisme et du séparatisme comme l'une des principales menaces pour la sécurité de l'État et des citoyens.

Donc, l'un des principaux domaines de la sécurité de l'information est la lutte contre l'utilisation des technologies de l'information pour propager l'idéologie extrémiste et répandre la xénophobie et les idées d'exclusivité nationale.

Les lois fédérales n° 398-FZ⁴ du 28/12/2013 et n° 327-FZ⁵ du 25/11/2017 ont complété la Loi fédérale n° 149-FZ par l'Article 15.3, qui régit la procédure de restriction de l'accès aux informations trouvées dans les réseaux d'information et de télécommunications, y compris l'Internet, contenant des appels aux émeutes, des activités extrémistes, la participation à des événements de masse (publics) organisés en violation de la procédure établie, ainsi que

² Ci-après SIAU (Système d'information automatisé unifié) « Registre unifié ».

³ Le Décret du Gouvernement de la Fédération de Russie n° 1101 du 26 octobre 2012 « Sur le système d'information automatisé unifié » Registre unifié des noms de domaine, des références aux pages web du réseau d'information et de télécommunication « Internet » et des adresses de réseau permettant d'identifier les sites du réseau d'information et de télécommunication « Internet » contenant des informations dont la diffusion est interdite dans la Fédération de Russie ». Ci-après le Décret n° 1101.

⁴ « Sur les modifications de la Loi fédérale » Sur l'information, les technologies de l'information et la sécurité de l'information ».

⁵ « Sur l'information, les technologies de l'information et la sécurité de l'information » et l'Article 6 de la Loi de la Fédération de Russie » Sur les médias de masse ».



des matériels d'information d'une organisation non gouvernementale étrangère ou internationale dont les activités sont en violation de la procédure établie, et des documents d'information d'une organisation non gouvernementale étrangère ou internationale dont les activités sont reconnues comme indésirables sur le territoire de la Fédération de Russie, ainsi que les données permettant

d'accéder à ces informations ou matériels.

Conformément à l'alinéa 1 de l'Article 15.3 de la Loi fédérale n° 149-FZ, lorsque les autorités fédérales, les autorités publiques des entités constitutives de la Fédération de Russie, les autorités locales, les organisations ou les citoyens reçoivent des notifications

de diffusion d'informations de cette nature sur les réseaux d'information et de télécommunications, y compris l'Internet, le Procureur général de la Fédération de Russie ou ses adjoints ont le droit de soumettre à Roskomnadzor une demande visant à prendre des mesures pour restreindre l'accès aux ressources d'information.

Roskomnadzor, à la base de la demande du Procureur général de la Fédération de Russie ou de ses adjoints, envoie immédiatement aux opérateurs de de télécommunications une demande de la prise de mesures visant à restreindre l'accès à une ressource d'information ou à des informations mises sur celle-ci, ensuite l'opérateur de télécommunications qui fournit des services d'accès au réseau d'information et de télécommunication « Internet » est tenu de limiter immédiatement l'accès à une telle ressource d'information. Les données sur la ressource d'information sont introduites par Roskomnadzor dans un registre séparé.

La procédure établie permet de répondre rapidement à la diffusion de telles informations sur l'Internet, ce qui est possible grâce à l'indication obligatoire dans la demande du Roskomnadzor du nom de domaine d'un site web sur Internet, de l'adresse de réseau, des liens aux pages du site web qui permettent d'identifier ces informations.



LES DERNIÈRES TENDANCES SUR LE MARCHÉ DES FOURNISSEURS ILLÉGAUX DE SERVICES FINANCIERS

Assurer la sécurité des revenus de la population et protéger les consommateurs contre la participation à des activités illégales sur le marché financier est l'un des objectifs les plus importants des régulateurs financiers



➤ **ROMAN MOUKHLYNOV,**
Directeur adjoint du Département
des prêts non bancaires de la Banque
Centrale de la Fédération de Russie

La Banque de Russie prend des mesures pour consolider les efforts de toutes les parties prenantes afin de protéger les épargnes des citoyens contre les fraudeurs et de résister aux pratiques trompeuses et illégales.

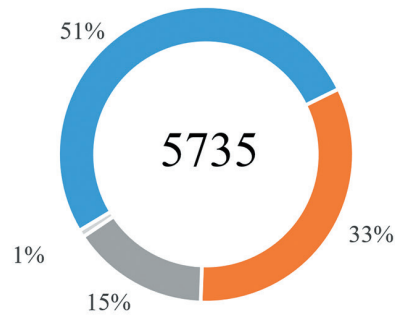
En 2023, la Banque de Russie a identifié 5 735 entités (entreprises, projets, entrepreneurs individuels et autres) présentant des signes d'activité illégale, y compris des signes de pyramides financières. C'est 15,5% de plus qu'un an plus tôt, mais la « durée de vie » de ces projets est devenue plus courte et le « panier moyen » a diminué. Les informations sur toutes les infractions identifiées pour la répression des activités illicites sont envoyées aux forces de l'ordre, Rosfinmonitoring, Service fédéral antimonopole de Russie, Roskomnadzor (Service fédéral de surveillance en matière des communications, technologies de

l'information et médias). Cependant, les fraudeurs utilisent chaque année de nouveaux projets et outils, et donc les autorités de régulation, les forces de l'ordre, les personnalités publiques et les établissements financiers doivent porter une attention accrue sur l'identification de telles pratiques.

Les tendances les plus importantes au cours des dernières années ont été la transition vers l'interaction en ligne et l'utilisation du thème des cryptomonnaies par des fraudeurs et des fournisseurs de services financiers illégaux. La Banque de Russie a souligné à plusieurs reprises que la prolifération des cryptomonnaies dans la Fédération de Russie comporte des risques élevés pour le bien-être des citoyens et la stabilité du système financier, ainsi que des risques d'implication des clients des établissements financiers dans des activités illégales, y compris la légalisation (le blanchiment)

► Distribution des entités portant des signes d'activité illégale en 2023

- Pyramides financières
- Créanciers illégaux
- Acteurs professionnels illégaux du marché des valeurs mobilières
- Autres formes



de capitaux et le financement du terrorisme¹. Pour faire face à cette situation, des recommandations ont été élaborées afin de réduire les risques pour les clients des banques et d'autres établissements financiers².

Le nombre croissant d'acteurs illégaux du marché financier qui attirent les investissements des crypto-monnaies est tout aussi dangereux. En 2022, les crypto-monnaies ont été utilisées par un projet d'investissements fictif sur deux. En 2023, presque tous les pyramides de Ponzi et des Forex Clubs illégaux proposaient des investissements dans des jetons internes ou acceptaient des contributions en crypto-monnaies.

L'utilisation de crypto-monnaies dans les activités illégales comporte des risques élevés en raison de la difficulté de tracer les transactions en crypto-monnaies, ce qui peut compliquer la recherche du bénéficiaire final d'un projet criminel. Les criminels s'adaptent rapidement aux nouvelles conditions, compliquant constamment les moyens de retirer des fonds de projets frauduleux de crypto-monnaies. Sur les 2 944 pyramides de Ponzi identifiées en 2023, plus de 45% ont offert aux « investisseurs » d'utiliser les systèmes de fournisseurs de services de paiement étrangers pour transférer des fonds. Près de 1 500 projets frauduleux ont accepté des contributions en crypto-monnaie,

ce qui permet notamment aux organisateurs et aux bénéficiaires de garder l'anonymat.

Dans le contexte d'une augmentation constante de l'intérêt des consommateurs pour l'obtention de services financiers à distance et du développement d'une confiance durable dans les informations obtenues à partir des médias sociaux, la plupart des pyramides financières, des pseudo-courtiers et même des créanciers illégaux travaillent en ligne, de sorte que de plus en plus de consommateurs peuvent être exposés à des pratiques trompeuses et à des fraudes.

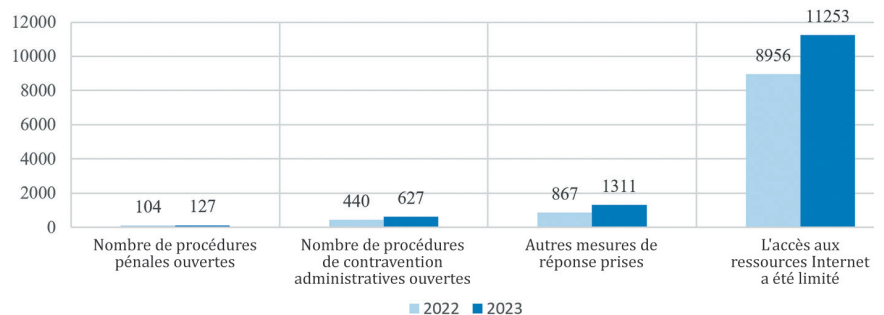
Bien sûr, la Banque de Russie améliore constamment la configuration du système de surveillance de l'espace d'information. Par exemple, l'année passée l'évaluation du contenu publié a été automatisée ; un an plus tôt, les réseaux sociaux et les

messageries instantanées ont été ajoutées au système de surveillance. Cela a permis d'améliorer la qualité et la rapidité de la détection des fournisseurs de services financiers illégaux. Les ressources illégales sont bloquées à l'initiative de la Banque de Russie, mais les organisateurs de ces projets créent de nouveaux services « en réponse ». Les fraudeurs créent souvent des ressources avec le même contenu après le blocage du site principal. À partir de 2023, afin de rendre le blocage plus complet, la Banque de Russie a commencé à prendre des mesures permettant de restreindre simultanément l'accès non seulement aux domaines, mais aussi à tous les sous-domaines utilisés par les entités d'activité illégale.

En 2023, à l'initiative de la Banque de Russie, l'accès à plus de 11 200 ressources Internet a été restreint, y compris les pages des réseaux sociaux VKontakte et Odnoklassniki et la messagerie Telegram (plus de 3 000 pages, chaînes, chatbots, etc.), qui étaient utilisés par des acteurs illégaux du marché financier et des pyramides de Ponzi. Le nombre total d'utilisateurs des ressources Internet bloquées s'élève à plus de 230 millions.

De plus, depuis 2022, nous avons commencé à ajouter des informations sur les entreprises illégales (personnes

► Mesures contre les organisations illégales et les pyramides financières prises à la demande de la banque de Russie



¹ Des informations sur les risques et les menaces associés à la prolifération des cryptoactifs (« monnaies virtuelles », crypto-monnaies) sont publiées sur le site officiel de la Banque de Russie sur Internet (le communiqué de presse du 27/01/2014 « Sur l'utilisation de « monnaies virtuelles », en particulier Bitcoin, lors de transactions » ; le communiqué de presse du 04/09/2017 « Sur l'utilisation de « monnaies virtuelles » privées (crypto-monnaies) » ; le rapport pour les consultations publiques du 20/01/2022 « Crypto-monnaies : tendances, risques, mesures »).

² Lettre d'information n° IN-08-12/18 du 29/02/2024 de la Banque de Russie parlant des risques de transactions avec des monnaies numériques et contenant des recommandations aux établissements financiers d'éliminer l'offre de services qui impliquent de telles transactions.

morales et entrepreneurs individuels) à la plateforme « Connaissance du client » afin que les banques puissent rapidement en tenir compte lors de l'évaluation du profil de risque de leurs clients et de leurs contractants, ainsi que pour appliquer des mesures « anti-blanchiment » à l'encontre des fournisseurs de services financiers illégaux. Actuellement, la plateforme comprend des informations sur environ 2 300 entités (pyramides de Ponzi, créanciers illégaux, Forex Clubs illégaux, etc.).

En outre, en 2023, les établissements de crédit ont obtenu des recommandations³, le cas échéant, d'appliquer des mesures « anti-blanchiment », jusqu'aux restrictions sur les transactions sur les comptes, à toutes les organisations figurant sur la Liste des sociétés présentant des signes d'activité illégale identifiée, qui est publiée sur le site officiel de la Banque de Russie, ainsi qu'à leurs intermédiaires. Cela diminuera la durée de vie des systèmes de Ponzi, rendra plus difficile la collecte de fonds par les fournisseurs de services financiers illégaux et réduira les dommages causés aux citoyens par les projets illégaux.

Par exemple, sur le marché de la microfinance, les prêts en ligne sont aujourd'hui très demandés par les clients : 75 % des contrats de prêt avec les institutions de microfinance, contre 66 % en 2022, sont conclus en ligne. En conséquence, le nombre de cas où des fraudeurs se font passer pour des emprunteurs afin de retirer de l'argent aux institutions de microfinance sous la forme de prêts non remboursés par la suite a augmenté. Il y a deux parties lésées dans ces projets.

Avant tout, les citoyens qui ont contracté des prêts frauduleux.

Ces prêts nuisent leurs dossiers d'emprunt, et il faut souvent beaucoup de ressources pour résoudre les difficultés. Deuxièmement, les institutions de microfinance, ce sont elles qui souffrent des pertes sous la forme de prêts non remboursés accordés à des fraudeurs, ainsi que des risques de réputation tout aussi importants. Le volume de ces attaques frauduleuses est assez élevé et a augmenté depuis 2022. En 2022-2023, le volume maximal des tentatives de fraude pour obtenir un prêt dans une seule grande institution de microfinance était d'environ 350 000-700 000 en termes de nombre de transactions; et d'environ 2-4 milliards de roubles en termes de volume de prêts. Il s'agit d'une intensité assez élevée et d'un montant potentiellement dommageable pour l'entreprise. La société a prévenu plus de 98% de ce genre de transactions. Toutefois, dans un avenir proche, les institutions de microfinance devront améliorer les procédures d'identification et de lutte contre la fraude lors de l'octroi de prêts en ligne. La Banque de Russie discute souvent ces questions avec les professionnels du secteur.

La loi⁴ a été élaborée afin de promouvoir la sécurité des consommateurs et de réduire les risques de fraude lors de l'octroi de prêts en ligne. Elle augmente la responsabilité financière des banques pour les transactions frauduleuses. En particulier, à partir de juillet 2024, a été introduit un délai de « réflexion » de deux jours pendant laquelle la banque ne transfère pas d'argent vers un compte suspect figurant dans la base de données de l'autorité de réglementation.

Pendant ces deux jours, une personne peut revenir à la raison, se rendre compte qu'elle a affaire à des fraudeurs et refuser le virement. Si la banque effectue un tel virement avant l'expiration du délai de réflexion, elle sera tenue d'indemniser le client pour la perte subie. En outre, la loi oblige les banques à désactiver l'accès aux services à distance pour les personnes qui retirent et encaissent de l'argent volé si des informations sur leurs actions illégales ont été reçues par le Ministère de l'Intérieur de Russie. De plus, les citoyens pourront s'assurer contre la situation où des fraudeurs font une demande de prêt à leur nom et refuser volontairement la conclusion des contrats de crédit ou de prêt. La loi entrera en vigueur le 1er mars 2025. À partir de cette date, il sera possible d'émettre ou d'annuler une auto-interdiction sur le portail « Services publics ». Toutefois, si, malgré l'interdiction, le créancier conclut un contrat, il ne pourra pas exiger de l'emprunteur qu'il remplisse ses obligations en vertu de ce contrat. L'auto-interdiction peut être annulée à tout moment si la personne a effectivement besoin d'un prêt ou d'un crédit.

Compte tenu du taux de croissance du format d'interaction à distance, de sa pénétration rapide dans la vie quotidienne des consommateurs de services financiers et le traitement médiatique des crypto-actifs et des monnaies numériques, la lutte contre ces pratiques trompeuses pourrait se déplacer presque entièrement vers le segment en ligne du marché financier.

³ Lettre d'information n° IN-08-12/69 du 27/12/2023 de la Banque de Russie sur l'attention soutenue des établissements de crédit aux transactions impliquant des personnes présentant des signes d'activités illégales sur le marché financier.

⁴ Loi fédérale n° 31 FZ du 26/02/2024 « Sur la modification de la Loi fédérale « Sur les dossiers d'emprunt » et à la Loi fédérale « Sur le crédit (prêt) à la consommation ».

L'UTILISATION DES TECHNOLOGIES NUMÉRIQUES DANS LA COLLECTE, LE TRAITEMENT ET LA GÉNÉRALISATION DES DONNÉES INFORMATIQUES ET ANALYTIQUE AINSI QUE D'AUTRES DONNÉES UTILISÉES DANS LES ACTIVITÉS DU PARQUET,

PAR EXEMPLE DANS LE CADRE DES FONCTIONNALITÉS DU SYSTÈME D'INFORMATION ET D'ANALYSE « BUREAU ÉLECTRONIQUE DU PROCUREUR »



OLEG KIPKAÏEV,
Chef du Service de la surveillance de l'application des lois dans le domaine des technologies de l'information et de la protection de l'information du Parquet général de la Fédération de Russie

En utilisant des technologies numériques modernes, le Bureau du procureur général de la Fédération de Russie travaille actuellement à l'élaboration d'un projet de système d'information et d'analyse intitulé « Bureau du procureur électronique » (ci-après dénommé « BPA ») afin de réduire les coûts de main-d'œuvre improductifs des procureurs liés à la collecte et au traitement de grandes quantités de données

Le développement de ce produit est due au besoin de reformater les modes traditionnels d'organisation des activités des procureurs dans le contexte de l'accélération de la transformation numérique des relations sociales qui nécessite l'introduction de nouveaux outils plus efficaces et plus rapides pour remplir à la fois des tâches analytiques et celles liées à la surveillance par le bureau du procureur. Parmi les principaux facteurs nécessitant des solutions informatiques et techniques innovantes, on distingue les éléments suivants :

- 1) **données** – le volume toujours croissant de données analysées crée pour les procureurs des difficultés supplémentaires qui sans l'introduction de moyens d'automatisation du travail, sont souvent insurmontables ;
- 2) **analyse** – la préparation de rapports et de résumés prend énormément de temps au détriment du travail quotidien des procureurs. Chaque année, il est de plus en plus difficile d'analyser toute l'information disponible ;

Problèmes

01 Données

Le volume toujours croissant de données analysées pose aux procureurs de nouvelles difficultés qui, sans l'introduction d'outils d'automatisation du travail, sont souvent insurmontables.

02 Analyse des données

La préparation de rapports et de résumés prend énormément de temps au détriment du travail quotidien des procureurs. Chaque année, il est de plus en plus difficile d'analyser toutes les données disponibles.

03 BigData (données massives)

Les parquets n'utilisent pas actuellement toutes les informations disposées par certains procureurs. En fait, elles sont prises en compte lors de la préparation de documents spécifiques, mais il est rare que leur potentiel soit pleinement exploité.

04 Contrôle

Les procureurs ont besoin d'informations précises sur les dates limites actuelles. Il n'est pas toujours pratique de travailler avec des listes de contrôle.

Intelligence artificielle simplification et normalisation

Préparation rapide de résumés
La description des infractions est normalisée et toujours à la main.



Analyse des infractions spécifiques
S'il est nécessaire de trouver tous les faits relatifs à la réponse aux infractions contre un acte réglementaire particulier à travers tout le pays, il suffit de faire une requête.



On n'a pas besoin d'un employé pour créer la base de données
Il est prévu que les actes de réponse soient simplement collectés dans un dossier par un agent autorisé, et le traitement sera automatique.



Élaboration de projets de rapports thématiques en un seul clic
Si le traitement de certains documents et le remplissage de la base de données sont efficaces, on peut passer à l'étape suivante : apprendre l'IA à générer de documents analytiques.



3) données massives – les parquets ne disposent pas de toutes les données opérées par certains procureurs. En fait, elles sont utilisées dans la préparation de documents séparés, mais rarement dans leur potentiel total ;

4) contrôle – les procureurs ont besoin d'informations visuelles sur les dates limites actuelles, il n'est pas toujours pratique de travailler avec des listes de contrôle.

Le concept du produit consiste en automatisation par des logiciels,

y compris en perspective par la technologie de l'intelligence artificielle, les processus de collecte, de traitement, d'accumulation, de généralisation et d'analyse des informations sur la légitimité et l'ordre, sur la pratique de la supervision et d'autres activités des procureurs.

Il est prévu d'utiliser comme unités de données primaires les actes de réponse du procureur, les rapports sur le remplissage des tâches et d'autres documents susceptibles d'être traités par des réseaux

neuronaux génératifs, notamment en extrayant les caractéristiques essentielles des fichiers texte correspondants. Il est prévu que les documents informatiques et analytiques sont générés automatiquement à partir du fichier de données chargé dans le système selon les paramètres spécifiés avec la possibilité de les mettre au point manuellement.

Par exemple, pour évaluer l'état de la surveillance dans le secteur des services de gestion des logements et des biens communaux, le

SAI CEM (Système d'analyse et d'information Calendrier électronique des missions) est capable de sélectionner toutes les présentations, contestations, actions en justice et autres actes qui contiennent des références à des violations de la loi dans ce domaine et fournir un rapport analytique avec des exemples à la fois concernant une région particulière et pour l'ensemble du pays.

Par ailleurs, l'accomplissement des tâches en cours pose certaines questions liées aux particularités du traitement automatique de textes pour lesquels on a besoin de trouver les décisions fondamentales.

La structure et le contenu des actes de réponse diffèrent souvent considérablement d'un parquet à l'autre, en fonction des pratiques locales, du style de présentation des informations et du surplus des extraits de lois dans les documents, y compris ceux qui ne sont pas directement liées aux violations signalées.

Cela constitue un obstacle au traitement intelligent des actes à l'aide de technologies informatiques basées sur les principes de l'apprentissage

automatique qui sont programmées pour travailler avec des données structurées unifiées par une logique de présentation de l'information, et nécessite la révision des exigences relatives à ces documents.

À l'avenir, l'utilisation de SAI CEM (Système d'analyse et d'information Calendrier électronique des missions) permettra de préparer les actes de la réponse du procureur, dont la structure sera unique pour tous les parquets, suivi de leur traitement par la machine et l'analyse, y compris les prévisions.

Les différents modules du système qui fonctionnent avec des données structurées qui n'exigent pas de traitement complexe, ont été mis en service en tant que projet pilote et sont en train d'être testés.

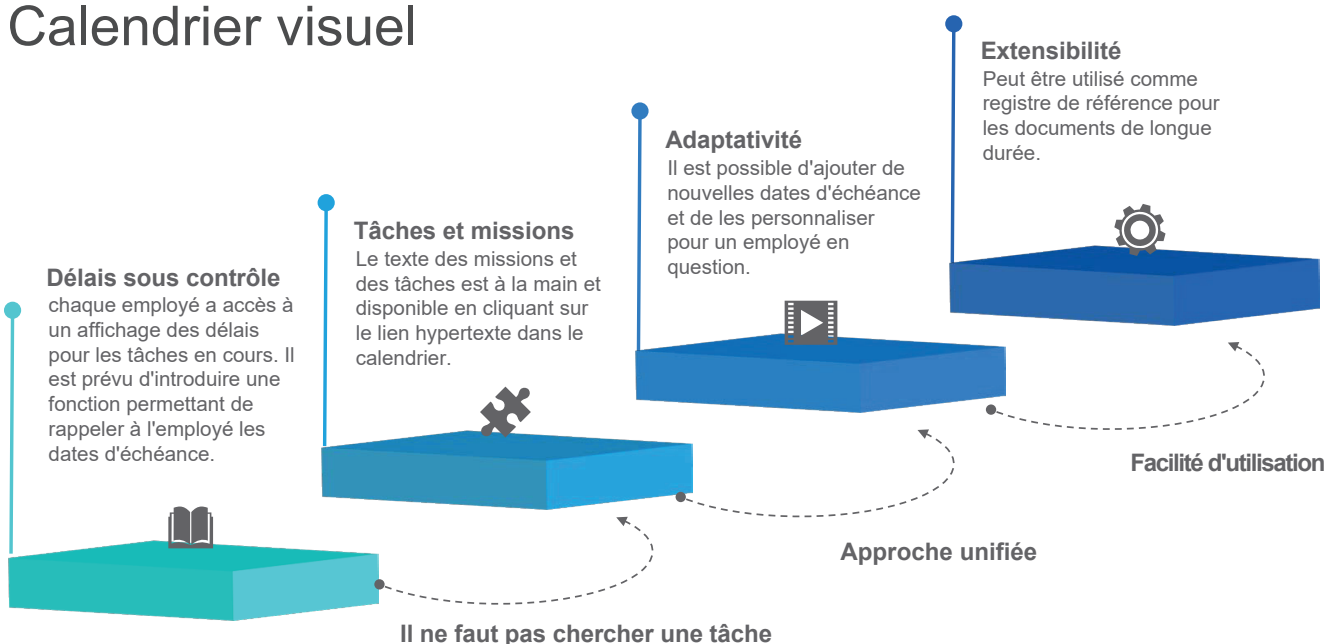
La fonction d'addition des indicateurs numériques (en un seul clic, avec vérification du contrôle logique) a été effectivement mise en œuvre, elle a été utilisée lors de la création de tableaux pour des tâches spécifiques ce qui a permis de constater une réelle simplification du travail quotidien et une réduction significative des délais de son exécution. Dans l'avenir,

l'utilisation d'outils électroniques de traitement des données avancés permettra d'informer d'une manière plus rapide les responsables du Bureau du procureur général sur l'état actuel et la dynamique des activités de la surveillance et d'autres, en particulier en l'absence de rapports, ce qui entre autres aura un impact positif sur la qualité des décisions de gestion.

Il existe également un composant SAI CEM (Système d'analyse et d'information Calendrier électronique des missions) qui est conçu non seulement pour contrôler la rapidité d'exécution des missions et de la recherche instantanée de leur origine, mais qui est également destiné à devenir un registre électronique officiel de toutes les tâches en cours d'exécution. Si un document n'y est pas inclus, il est considéré comme non exécutable. Cette fonction vise également à diminuer la charge d'organisation du travail, par conséquent, à libérer la main-d'œuvre pour s'acquitter des tâches de supervision du parquet.

Le calendrier offre la possibilité de l'utiliser à tous les niveaux des parquets.

Calendrier visuel



La première région qui a introduit cette fonctionnalité était celle de Kourgan. Les employés du parquet concerné ont profité de la possibilité de créer des liens hypertextes vers les documents enregistrés dans le Système d'Information Automatisée Nadzor-WEB (la surveillance web). Ainsi, il est possible non seulement de consulter les informations relatives au délai d'exécution, mais aussi d'accéder rapidement au document qui l'a fixé.

En ce qui concerne les rapports sur les activités, la création d'un modèle électronique, structuré selon les blocs logiques et thématiques d'une tâche ou d'une mission, dont le contenu (afin de le rendre concis) est limité en nombre de caractères imprimés, et d'autres paramètres sont définis pour remplir le modèle afin d'améliorer la recherche rapide de l'informations et son traitement est en cours d'approbation.

Cette approche permettra de :

- 1) fournir un stockage sûr, la possibilité d'utiliser la fonctionnelle analytique, et à l'avenir, les données collectées pourront être utilisées pour l'apprentissage de l'intelligence artificielle (les informations sont stockées dans la base de données) ;
- 2) faire une recherche instantanée sur les rapports recueillis, améliorer l'efficacité d'utilisation des données accumulées, ainsi que leur stockage (recherche approfondie) ;
- 3) enregistrer l'historique des messages sur le sujet d'analyse, c'est-à-dire que lors du changement de personnel, tous les rapports sur la surveillance seront disponibles pour le nouvel employé (continuité du travail d'analyse) ;
- 4) regrouper les données des rapports par sections thématiques selon la structure établie, ce qui facilitera le traitement de l'information en

fonction du volume de la tâche d'analyse (simplification de la généralisation des rapports selon des paramètres spécifiés).

Le SAI CEM comprend des modules spécialisés qui ont été exploités avec succès et sont déjà devenus un outil important dans les activités du parquet, en particulier le « Registre des ressources Internet contenant des informations illégales » (ci-après dénommé le Registre, le RRII).

Dans une lettre du premier Procureur général adjoint de la Fédération de Russie datée du 12 avril 2023 « Amélioration des résultats de préparation des conclusions et des requêtes administratives visant à bloquer les informations diffusées en violation de la loi sur Internet », les procureurs sont invités à utiliser le Registre afin de vérifier les adresses des sites Internet et d'éviter la répétition des mesures de réponse prises.

Avant de la mise à la disposition du Registre, lors de la préparation des conclusions envoyées au Parquet général de la Fédération de Russie sur les ressources Internet contenant des propositions d'obtention de faux papiers, conférant des droits ou exonérant des obligations, l'efficacité de la réponse du procureur ne dépassait pas 15 %. Cela était dû à la duplication des sites qu'ils proposaient d'inclure dans l'obligation de prendre des mesures pour y restreindre l'accès.

Par exemple, 10 procureurs pouvaient signaler la même ressource : diplom.com. Pour ce faire, chaque intervenant passait du temps à vérifier et à préparer le paquet de documents requis.

Après avoir commencé à utiliser le RRII, l'efficacité de certains procureurs dans le domaine en question a augmenté de 50 à 70 %. Si tous les procureurs utilisent le

ressource approprié, ce chiffre devrait atteindre 95 %.

Le registre des contrats publics conclus dans le cadre du projet national « Économie numérique » joue actuellement un rôle important dans l'amélioration de la qualité des activités de surveillance. Ce registre qui fait partie du SAI CEM, permet aux procureurs d'obtenir des informations sur les contrats administratifs conclus sur le territoire contrôlé dans le cadre du projet national susmentionné, sans demandes supplémentaires. La source d'information est Rosfinmonitoring (Service fédéral de surveillance financière), les données sont mises à jour chaque trimestre.

Des informations sur les possibilités dudit registre ont été communiquées aux procureurs subordonnés dans la lettre d'information du premier Procureur général adjoint de la Fédération de Russie datée du 31/07/2023 « Sur le renforcement de la surveillance exercée par les procureurs dans l'application de la législation dans le cadre de la mise en œuvre du projet national « Économie numérique ».

Ainsi, la plateforme du SAI CEM peut déjà être considérée comme un véritable assistant électronique pour les procureurs à tous les niveaux, et à l'avenir, la mise au point de ce produit avec tout son potentiel peut changer radicalement les méthodes traditionnelles d'organisation des activités du parquet, en basculant leur travail depuis l'exécution de tâches purement techniques vers le traitement direct intellectuel des données, et, par conséquent, améliorer la qualité de la surveillance et l'état de la garantie des droits et libertés des citoyens.



CRYPTO-MONNAIE : À LA RECHERCHE DE SOLUTIONS

68 OLGA TISENE

Réglementation juridique de la circulation des actifs virtuels et de la lutte contre leur utilisation à des fins LBC/FT dans des pays de l'EAG

73 DMITRI MATCHIKHINE

Enquêtes LBC dans l'industrie Web-3

77 SEAN MOUNIR

Travail avec les actifs numériques : cryptomonnaie, NFT et sécurité financière

RÉGLEMENTATION JURIDIQUE DE LA CIRCULATION DES ACTIFS VIRTUELS ET DE LA LUTTE CONTRE LEUR UTILISATION À DES FINS LBC/FT DANS DES PAYS DE L'EAG

La technologie du registre distribué et les relations dans ce domaine ont été considérablement transformées durant leurs 15 années d'existence. Maintenant, des mélangeurs, des mixeurs et des proxy anonymiseurs sont apparus permettant de cacher les liens d'un propriétaire particulier avec les transactions, une infrastructure développée de prestataires de services d'actifs virtuels (ci-après le PSAV)¹ a été formée, y compris ceux qui travaillent dans le secteur parallèle, alors que le nombre de crypto-monnaies a augmenté à plusieurs reprises



▶ OLGA TISENE,
Cheffe du Département juridique de Rosfinmonitoring, docteur en droit, coprésident du Groupe de travail sur les évaluations mutuelles et les questions juridiques de l'EAG

Le premier document au niveau international consacré aux nouveaux objets numériques a été le rapport du Groupe d'action financière (GAFI) « Les monnaies virtuelles », publié en juin 2014². Il avait des définitions clés relatives à l'exploitation d'actifs virtuels et aux risques dérivés établis à l'époque. Il a également été noté que les monnaies virtuelles entre les mains de criminels deviennent un nouvel outil puissant pour déplacer et conserver de l'argent hors de portée des forces de l'ordre et d'autres autorités compétentes.

Un an plus tard, en juin 2015, le GAFI a publié le Guide d'application de l'approche fondée sur les risques pour les actifs virtuels. Il décrit les principaux moyens de minimiser les risques d'utilisation des monnaies numériques à des fins de blanchiment de capitaux et de financement du terrorisme.

En octobre 2018, les normes du GAFI ont été appliquées aux activités financières liées aux actifs virtuels. Les Recommandations du GAFI sont mises à jour chaque année depuis 2021. En 2020, le GAFI a publié le rapport sur les indices de blanchiment de capitaux et de financement du terrorisme dans la circulation des actifs virtuels, ainsi qu'un rapport aux ministères des Finances et aux banques centrales des pays participants du G20 concernant les stablecoins (cryptomonnaie stable)³.

Avec l'adoption de ces documents, une base juridique internationale a été formée pour établir des régimes dans les États en ce qui concerne le trafic des AV (actifs virtuels) afin de contrer les menaces à la sécurité comprenant l'utilisation de crypto-monnaie⁴ par la criminalité transnationale organisée, y compris

¹ Les PSAV sont les prestataires de services d'actifs virtuels : toute personne physique ou morale qui effectue, en tant qu'entreprise, une ou plusieurs des transactions suivantes pour/ou de la part d'une autre personne physique ou morale : échange entre actifs virtuels et monnaies fiduciaires ; échange entre une ou plusieurs formes d'actifs virtuels ; transfert d'actifs virtuels ; conservation et/ou administration d'actifs virtuels ou d'instruments permettant de contrôler les actifs virtuels ; participation et fourniture de services financiers liés à l'offre et/ou à la vente de l'actif virtuel // Monnaies virtuelles. Définitions clés et risques potentiels en matière de LBC/FT : rapport du GAFI, juin 2014.

² Monnaies virtuelles. Définitions clés et risques potentiels en matière de LBC/FT : rapport du GAFI, juin 2014 // www.fatf-gafi.org

³ www.fatf-gafi.org

⁴ Dans le cadre du présent article, la crypto-monnaie désigne une monnaie virtuelle convertible décentralisée. Les termes « crypto-monnaie », « actifs virtuels », « crypto-actifs » ont la même signification dans cet article.

aux fins de la légalisation (blanchiment) de capitaux et du financement du terrorisme⁵.

IL EST ÉVIDENT QUE L'INTRODUCTION D'UNE RÉGLEMENTATION DES PSAV, L'APPLICATION DES EXIGENCES CONCERNANT LES NORMES INTERNATIONALES DE LBC/FT À CES DERNIERS OU L'INTERDICTION TOTALE DES ACTIFS VIRTUELS EST UNE RÉALITÉ INCONTOURNABLE POUR TOUS LES ÉTATS.

Les principales exigences des normes du GAFI en matière de la circulation des actifs virtuels :

- Les États sont tenus d'identifier, d'évaluer et d'atténuer les risques de BC/FT découlant des transactions des actifs virtuels (ci-après dénommés « AV ») ;
- aux fins d'application des normes du GAFI, les AV doivent être classés comme des biens, ce qui signifie qu'ils font l'objet d'infractions, y compris les infractions liées à BC/FT. Les AV ayant le statut de biens sont soumis au blocage (gel), à la saisie et à la confiscation ;
- les activités des PSAV qui effectuent des transactions d'échange avec des AV, le virement des actifs virtuels et leur conservation doivent être contrôlées, notamment par l'enregistrement/l'octroi de licences et la surveillance de ces personnes. Les PSAV doivent être chargés d'identifier les clients et leurs bénéficiaires effectifs, de signaler les transactions suspectes à la cellule de renseignement financier et de stocker les données.

Le Guide d'application de l'approche fondée sur les risques concernant les AV et les PSAV établi par le GAFI en octobre 2021 explique que les pays peuvent interdire ou restreindre les activités liées aux AV ou la fonctionnalité des PSAV en fonction de l'évaluation des risques et de la législation nationale, ainsi que d'autres objectifs politiques tels que la protection des consommateurs, la sécurité et la stabilité, la politique monétaire⁶. En cas de prise de décision d'interdire ou de restreindre les activités avec des AV dans un pays, les dispositions de la Recommandation 15 du GAFI ne sont pas applicables à ce sujet, mais les juridictions seront tenues d'évaluer les risques qui en découlent. En cas de violation de l'interdiction de la circulation des AV, les États qui ont pris une telle décision doivent prendre des mesures appropriées à l'encontre des malfaiteurs (paragraphes 108 et 109 du Guide) et identifier les personnes physiques et morales qui exercent des activités dans ce domaine sans enregistrement et licence.

La résolution 1617 du Conseil de sécurité des Nations unies insiste sur la nécessité de se conformer aux normes du GAFI et aux normes internationales universelles spécifiées dans les 40 recommandations du Groupe d'action financière sur le blanchiment de capitaux et les 9 recommandations sur le financement du terrorisme.

En ce qui concerne l'approche de la réalisation de la Recommandation 15 du GAFI on distingue 3 modèles de réglementation de la circulation des actifs virtuels :

- 1) interdiction de la circulation des actifs virtuels dans le pays et de leur utilisation comme moyen de paiement ;

- 2) approche permissive : légalisation de la circulation des AV sur le territoire du pays, y compris en tant que moyen de paiement, établissement d'un marché et création d'une infrastructure appropriée ;

- 3) réglementation de la circulation des AV en imposant des restrictions législatives à son utilisation et la réglementation des activités des PSAV. Ce modèle est le plus répandu dans le monde entier.

La plupart des pays ont déjà adopté des normes qui définissent le statut légal des AV au sein de la juridiction : interdiction/autorisation de les utiliser comme moyen de paiement, option de posséder des AV et de les investir, etc. Toutefois, la classification législative des PSAV en tant qu'entités de LBC/FT pour lutter contre l'utilisation des crypto-monnaies par les criminels progresse plus lentement dans de nombreux États.

Les trois modèles décrits sont utilisés dans les pays de l'EAG. Ainsi, en Chine continentale, en 2017, une interdiction de l'utilisation de la crypto-monnaie a été introduite. Les PSAV sont déjà classés comme les entités LBC/FT en Biélorussie, en Inde, au Kazakhstan, au Kirghizistan et en Ouzbékistan. La réglementation des activités des FSAN⁷ est établie pour les entités situées en Fédération de Russie. Le Tadjikistan et le Turkménistan sont en train d'élaborer de telles normes.

RÉPUBLIQUE DU BÉLARUS

Le statut légal de la circulation des AV au Bélarus a été introduit en 2017 par le Décret no 8 du Président de la République du Bélarus du 21/12/2017 « Sur le développement

⁵ Annexe à l'Arrêté no 15-6.5 du 05/12/2022 de l'Assemblée parlementaire de l'Organisation du traité de sécurité collective

⁶ www.fatf-gafi.org

⁷ FSAN est le fournisseur de services d'actifs numériques

de l'économie numérique⁸ » (ci-après « le Décret »). Le document vise à créer les conditions basées sur les principes de distribution, de décentralisation et de sécurité des transactions effectuées avec aide de la blockchain et d'autres technologies pour les introduire dans l'économie de la République.

Selon l'annexe 1 du Décret, la crypto-monnaie est le bitcoin et un autre caractère numérique (token) utilisé en circulation internationale comme moyen d'échange universel.

Selon la législation de la République du Bélarus, les citoyens du pays ont le droit d'acheter et de vendre des crypto-monnaies sur n'importe quelle plateforme d'échange de crypto-monnaies, y compris les plateformes internationales. Pour leur part, les personnes morales ne peuvent travailler qu'avec des résidents du Parc de haute technologie⁹. Les entrepreneurs individuels ont le droit d'effectuer des transactions d'acquisition ou d'aliénation de crypto-monnaies, s'ils sont résidents du PHT (sous-paragraphe 2.2 du Décret).

L'activité entrepreneuriale suivante est illégale et interdite aux personnes physiques et morales qui ne sont pas résidents du PHT : assistance à d'autres personnes sur le territoire de la République du Bélarus et (ou) en utilisant l'Internet dans la réalisation et (ou) l'exécution des transactions (opérations) avec des tokens (y compris agir en tant que partie dans de telles transactions (opérations)) en utilisant le système d'information fonctionnant sur Internet ou en accordant le droit (l'autorisation) à d'autres personnes de l'utiliser, ainsi que l'acquisition et (ou) l'aliénation, y compris l'échange de tokens (sous-paragraphe 2.6 du paragraphe 2 du Décret).



Les activités des PSAV dans le pays sont réglementées par l'Administration du PHT, la Banque nationale de la République du Bélarus et le Comité de contrôle de l'État. Il est interdit de contrôler les résidents du Parc de haute technologie sans approbation préalable de l'Établissement public « Administration du Parc de haute technologie » (paragraphe 4.6 du Décret).

D'après la législation, les types d'activités entrepreneuriales suivantes sont autorisées en Biélorussie sur le territoire du PHT pour les résidents du PHT, qui, selon les normes du GAFI, appartiennent aux PSAV : plateforme d'échange de crypto-monnaies, bureau de change de crypto-monnaies, organisateur d'ICO, pool de minage.

Toutes les PSAV opérant sur le site du PHT sont désignés comme des entités de LBC/FT et sont tenus de mettre en œuvre des procédures pour respecter les exigences en matière de blanchiment d'argent.

RÉPUBLIQUE DU KAZAKHSTAN

La réglementation de la circulation des actifs virtuels dans la République du Kazakhstan établie par la Loi no 347-VI ZRK du 25/06/2020 « Sur les

modifications et les compléments dans certains actes législatifs de la République du Kazakhstan en matière de réglementation des technologies numériques », selon laquelle les actifs numériques ont été reconnus comme des biens, mais leur utilisation comme moyen de paiement sur le territoire du Kazakhstan est interdite.

La loi sur les crypto-monnaies classe les actifs numériques en deux catégories : les actifs garantis et les actifs non garantis. Les crypto-monnaies sont assimilées à des actifs non garantis, leur émission et leur circulation sont interdites au Kazakhstan, sauf sur le territoire du Centre International des Finances d'Astana (CIFA) fondé en 2018.

Le 18/11/2021, la Loi de la République du Kazakhstan n° 73-VII ZRK « Sur les modifications et les compléments à certains actes législatifs de la République du Kazakhstan sur la lutte contre le blanchiment de capitaux et le financement du terrorisme » a été adoptée. En vertu de cette loi, les personnes exerçant des activités liées à l'émission d'actifs numériques, à l'organisation d'appels d'offres de ces actifs, ainsi qu'à la fourniture de services pour l'échange d'actifs numériques contre de l'argent, des objets de valeur et d'autres biens, sont considérées

⁸ <https://president.gov.by/ru/documents/dekret-8-ot-21-dekabrya-2017-g-17716>

⁹ Ci-après PHT (Parc de haute technologie), le Parc

comme des entités de surveillance financière. Ces entités sont tenues de notifier à l'autorité compétente dans le domaine de l'informatisation le début et la fin de leurs activités, ce qui est porté sur le registre national approprié.

La loi de la République du Kazakhstan n° 53-VII ZRK datée du 24/06/2021 « Sur les modifications et les compléments au Code de la République du Kazakhstan « Sur les impôts et autres prélèvements obligatoires au budget » (Code des impôts) et la Loi de la République du Kazakhstan « Sur la mise en application du Code de la République du Kazakhstan « Sur les impôts et autres prélèvements obligatoires au budget » (Code des impôts) » » réglemente l'imposition de l'exploitation du minage numérique.

Afin de développer l'industrie des actifs numériques, le 06/02/2023 le Président a signé la loi de la République du Kazakhstan « Sur les actifs numériques dans la République du Kazakhstan » (ci-après la Loi) qui introduit le contrôle de l'État sur l'octroi de licences et l'administration, ainsi que l'imposition fiscale des actifs numériques.

Le Ministère du développement numérique, des innovations et de l'industrie de la construction spatiale de la République du Kazakhstan est l'autorité compétente pour déterminer le régime juridique de la vente des actifs numériques. D'après la loi sur les actifs numériques, l'émission et la circulation d'actifs numériques non garantis et les activités d'échange d'actifs numériques non garantis sont

interdites sur le territoire de la République du Kazakhstan, à l'exception du territoire du CIFA. Dans le cadre du CIFA, la réglementation des fournisseurs de services d'actifs numériques ainsi que la circulation des actifs numériques s'effectuent dans un « bac à sable » réglementaire.

Outre la circulation des actifs numériques, les actes du CIFA réglementent un large éventail de fournisseurs de services d'actifs numériques (FSAN), y compris les plateformes d'échange de crypto-monnaies, les courtiers, les agents de change, les conservateurs des titres, les gérants de fonds et les conseillers.

Afin d'éviter que les FSAN ne soient utilisées à des fins de blanchiment de capitaux et de financement du terrorisme, ils sont tenus d'assurer le fonctionnement des systèmes de contrôle clés suivants : « Connaissance du client » (ou « know your customer ») et « Connaissance de votre transaction » (ou « know your transaction »). C'est-à-dire, les FSAN procèdent à l'identification et au contrôle approprié non seulement de chaque client, mais vérifient également leur portefeuille numérique personnel et l'historique de leurs transactions pour y trouver des signes de violation de la législation contre le blanchiment d'argent et le financement du terrorisme.

L'Article 3 de la Loi de la République du Kazakhstan « Sur la lutte contre la légalisation (le blanchiment) de capitaux et le financement du terrorisme » classe les personnes qui émettent des actifs numériques, organisent des transactions avec ces actifs et fournissent des services d'échange d'actifs numériques contre de l'argent, des objets de valeur et d'autres biens comme des entités soumises à une surveillance financière. L'ordonnance du Président de l'Agence de surveillance





financière de la République du Kazakhstan « Sur l'approbation des règles de présentation par les entités de la surveillance financière des données et des informations sur les transactions soumises à la surveillance financière et les signes de définition de la transaction suspecte » établit les signes de définition de la transaction suspecte dans le domaine des actifs numériques.

Au Kazakhstan, une attention particulière a été accordée à la réglementation des activités des pools de minage attribués par les normes du GAFI au PSAV¹⁰.

RÉPUBLIQUE KIRGHIZE

La Loi n° 12 du 21/01/2022 de la République Kirghize « Sur les actifs virtuels » est entrée en vigueur le 28/07/2022. La loi comprend les termes principaux relatifs au domaine réglementée, le statut légal des actifs virtuels et les exigences envers les acteurs de la circulation des crypto-monnaies.

Les entités suivantes impliquées dans la circulation des crypto-monnaies ont été sélectionnées en République kirghize : prestataires de

services d'actifs virtuels, opérateurs d'appels d'offres d'actifs virtuels, plateformes d'échange de crypto-monnaies et pools de minage¹¹.

Conformément au paragraphe 19 de l'Article 5 de la Loi n° 87 du 06/08/2018 « Sur la lutte contre le financement du terrorisme et la blanchiment de capitaux »¹² (ci-après la Loi n° 87) les PSAV sont des établissements financiers tenus de vérifier les clients, de signaler les transactions suspectes au Service national de renseignement financier auprès du ministère des Finances de la République kirghize, de déclarer les transactions suspectes et de remplir d'autres fonctions dans le cadre du contrôle interne afin de lutter contre le blanchiment de capitaux et le financement du terrorisme.

Conformément aux Articles 16, 18, 25 et 28 de la Loi de la République kirghize « Sur les actifs virtuels », la résolution du Conseil des ministres de la République kirghize n° 514 du 16/09/2022 « Sur la réglementation des relations découlant de la vente d'actifs virtuels » a été adoptée. La loi n° 87 a été modifiée par l'Article 2 de la Loi n° 81 du 05/08/2022 « Sur la modification de certains actes législatifs dans le domaine des actifs virtuels ». Les PSAV sont

classés comme des établissements financiers, et toutes les exigences énoncées dans la Loi n° 87 concernant les Recommandations 10-21 du GAFI s'appliquent aux PSAV.

Les activités des PSAV au Kirghizstan sont soumises à l'octroi de licences. Les licences sont délivrées par le Service de réglementation et de surveillance du marché financier auprès du ministère de l'Économie et du Commerce du Kirghizstan. Les fournisseurs de services d'actifs virtuels doivent être exclusivement des personnes morales enregistrées dans le pays.

La coopération du Service national de renseignement financier de la République kirghize avec les opérateurs de systèmes de paiement électronique s'effectue conformément à la Loi n° 87 et à la Disposition sur la procédure de présentation d'informations et des documents de l'autorité de renseignement financier de la République kirghize (approuvé par l'Arrêté du Gouvernement de la République kirghize n° 606 du 25/12/2018). Les VASP doivent se conformer à cette Disposition lors de la procédure « Connaissance du client ».

15 ans après la création des crypto-monnaies se sont écoulés et il est clair que les lacunes en droit de leur circulation créent des menaces supplémentaires pour la sécurité économique et multiplient les risques de leur utilisation pour commettre des crimes.

La suite de l'article sur la réglementation de la circulation de la crypto-monnaie dans d'autres pays de la CEI et des BRICS sera disponible dans la prochaine édition de la revue.

¹⁰ P. 5 de l'Art. 11 de la Loi de la République du Kazakhstan « Sur les actifs financiers numériques » // https://online.zakon.kz/m/document/?doc_id=33689356

¹¹ <http://cbd.minjust.gov.kg/act/view/ru>.

¹² <http://cbd.minjust.gov.kg/act/view/ru-ru/111822?ysclid=loiruxojbb75473943>.

ENQUÊTES LBC DANS L'INDUSTRIE WEB-3

Au cours des dix dernières années, le monde financier a été considérablement transformé par l'émergence des crypto-monnaies. En fait, il s'agit de l'émergence d'un nouveau système financier parallèle. Il est évident, bien sûr, que les transactions illégales ne représentent pas 100% dans ce système (en réalité pas plus de 0,5% sont illégales), le nombre d'infractions est quand même très grand



DMITRI MATCHIKHINE,
Expert international en paiements
et AML (LBC/FT) dans le domaine
de Web3.
Membre du Conseil d'experts de la
légalisation de la crypto-monnaie
près de la Douma d'État de la
Fédération de Russie

Il s'agit principalement du blanchiment de capitaux (Anti-Money Laundering, lutte contre le blanchiment de capitaux ci-après « LBC »), du financement du terrorisme, de diverses formes de fraude, de piratage informatique et de détournement de fonds. Des outils technologiques de surveillance, d'investigation et de lutte contre ces menaces sont créés et déployés avec succès.

Dans cet article, nous examinerons les avantages et les inconvénients des solutions de lutte contre le blanchiment de capitaux existantes

sur le marché des crypto-monnaies, nous présenterons diverses méthodes d'identification des propriétaires d'adresses Bitcoin et nous évaluerons la fréquence d'utilisation des actifs virtuels à des fins criminelles.

COMMENT ET QUAND LBC A DIRECTEMENT AFFECTÉ LES CRYPTOMONNAIES ?

Tout au début du Bitcoin et d'autres cryptoactifs, LBC n'existait pas du tout dans ce domaine. C'est à cette époque que sont apparues les marchés en ligne-darknet anonymes, comme Silk Road.

Des actes législatifs généraux (droit administratif, pénal, fiscal, etc.) ont été utilisés comme des dispositions réglementaires, alors que personne n'a été impliqué dans le suivi et la vérification des transactions en ligne. À leur tour, les places de marché légales ont déterminé indépendamment le besoin d'identifier leurs clients via KYC (en anglais Know Your Customer) en appliquant la réglementation du marché financier de la même manière.

C'est ainsi que, conscient de l'urgence du problème et de la popularité croissante des crypto-monnaies, et grâce à la découverte et à l'arrestation des fondateurs de Silk Road en juin

2014, le Groupe d'action financière (GAFI,) a identifié pour la première fois les risques associés au marché des crypto-monnaies.

C'est alors que le GAFI a publié le rapport¹ « Virtual Currencies : Key Definitions and Potential AML/CFT Risks », qui décrit les risques potentiels de blanchiment de capitaux par le biais de cryptomonnaies.

Et seulement cinq ans plus tard, en 2019, le GAFI a présenté les premières recommandations qui ont affecté non seulement les sites qui traitent des actifs virtuels, mais aussi les crypto-monnaies elles-mêmes.

Dans les directives, l'organisme de réglementation a déterminé les principes de base LBC du marché des crypto-monnaies et les pouvoirs des autorités publiques dans ce domaine.

LES INFRACTIONS EN CRYPTO, LEUR FRÉQUENCE ET LEUR RÔLE

Malgré leurs propriétés prometteuses en matière de démocratisation des marchés financiers, les crypto-monnaies sont également devenues très répandues dans les milieux criminels. Divers jetons, y compris Bitcoin lui-même, sont souvent utilisés pour un large éventail de crimes.

¹ Virtual Currencies : Key Definitions and Potential AML/CFT Risks [Ressource électronique] // FATF. - Mode d'accès : <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.coredownload.pdf> (date de référence : 20/02/2024)

² Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers [Ressource électronique] // FATF. - Mode d'accès : <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets.html> (date de référence : 20/02/2024)

La crypto-monnaie est utilisée pour légaliser le produit du crime, de la fraude et de l'extorsion. Dans ce cas les malfaiteurs ont le plus souvent recours à des stablecoins dépourvus de risque de volatilité et ayant la même valeur que le dollar américain, comme Tether (USDT) ou USD Coin (USDC).

Les malfaiteurs profitent souvent des célébrités pour gagner la confiance de la victime. À la fin de 2023, des inconnus ont pu voler aux victimes plus de 160 000 \$ sur différents réseaux de blockchain, en se faisant passer pour un entrepreneur américain via le service vidéo YouTube.

L'anonymat accru des certaines cryptomonnaies les rend attrayantes pour les transferts transfrontaliers entre criminels. Toutefois, la tendance est à³ la réglementation stricte et à l'attention portée à ces actifs à l'échelle mondiale.

Ainsi, selon la plateforme⁴ américaine d'analyse de la blockchain Chainalysis,

depuis 2017, les crypto-monnaies ont été le plus souvent mises en avant dans des schémas frauduleux.

Cependant, on ne peut pas affirmer que les crypto-monnaies en général ne sont pas utilisées pour le financement du terrorisme. Malgré de nombreuses mesures pour mettre fin à cette activité, il y a eu des cas particuliers où les efforts déployés n'ont pas été suffisants.

COMMENT LES CRYPTO-MONNAIES « SALES » SONT-ELLES TROUVÉES ET QUE SE PASSE-T-IL SI SEULES LES ADRESSES SONT CONNUES ?

Diverses méthodes d'identification et d'analyse des transactions de la blockchain sont utilisées pour identifier les activités illégales de crypto-monnaies. Cependant, le résultat des enquêtes dépend non seulement des techniques d'investigation utilisées par le fournisseur LBC, mais aussi des actions des cybermalfaiteurs.

Les fournisseurs LBC utilisent différentes méthodes pour identifier les moyens « sales ». Par exemple, l'une des techniques connues consiste à pulvériser⁵ (dust attack en anglais) un petit volume de crypto-monnaie sur les adresses ciblées afin d'identifier plus tard l'identité du propriétaire de l'adresse.

Les employés de la société d'analyse Chainalysis et CipherTrace avaient déjà réfuté en publique⁶ l'utilisation de ces technique dans leur travail. Ils ont toutefois reconnu que certains analystes de blockchain ont eu recours à de telles méthodes d'analyse.

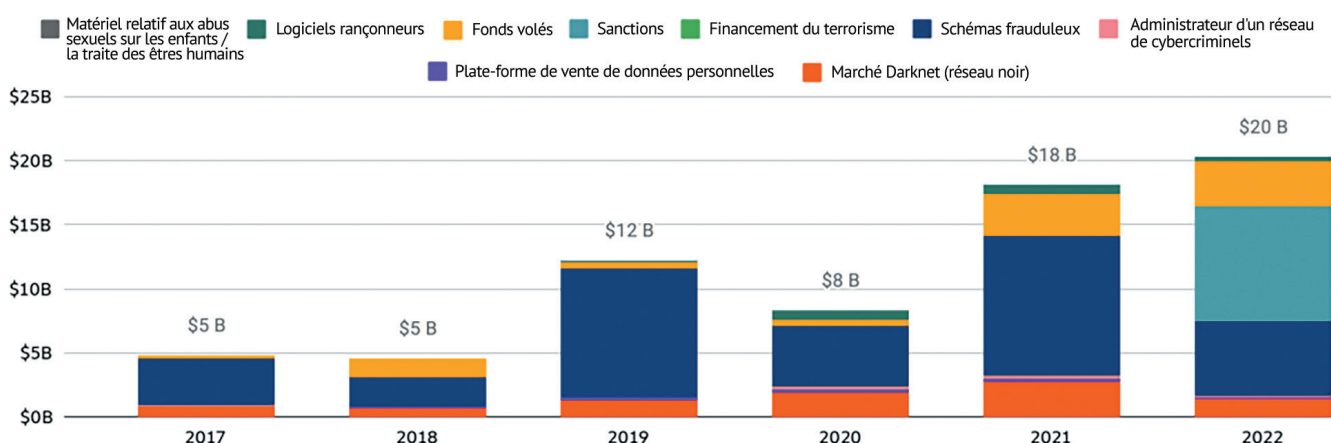
Cependant, l'analyse des données de blockchain ne se limite pas à elle seule. Les grands fournisseurs de LBC ont tendance à posséder un personnel d'experts en analyse de blockchain et en criminalistique qui identifient les adresses de crypto-monnaie de manière déterministe.

Par exemple, dans le cas des services de crypto-monnaie, les analystes identifient les adresses

► Répartition des volumes de crypto-monnaies reçues sur les adresses « sales » par catégorie

Source : Chainalysis

Valeur totale des crypto-monnaies reçues aux adresses (portefeuilles) des criminels, 2017-2022



³ Binance Will Delist ANT, MULTI, VAI, XMR on 2024-02-20 [Ressource électronique] // Binance. - Mode d'accès : <https://www.binance.com/en/support/announcement/binance-will-delist-ant-multi-vai-xmr-on-2024-02-20-f73b083ba6834771b07dbe5319917ae5> (date de référence : 20/02/2024)

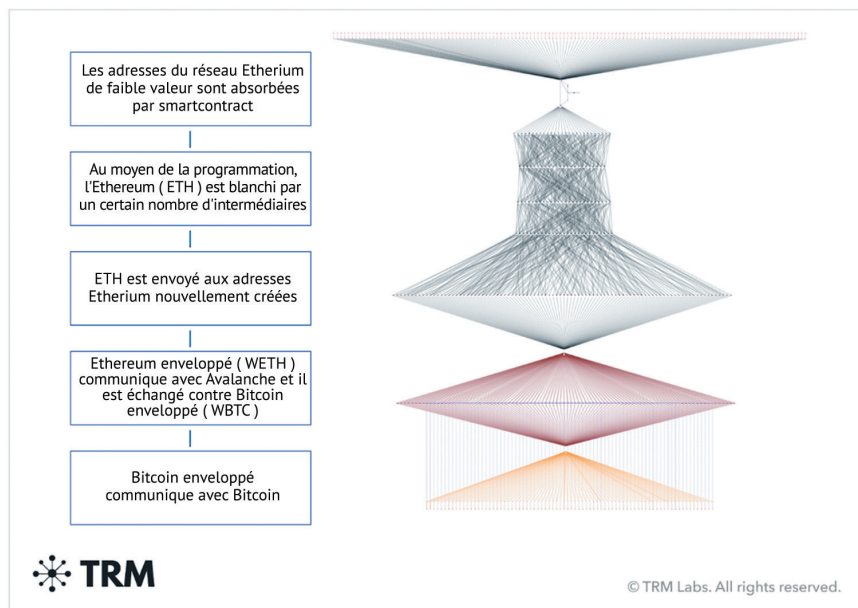
⁴ 2023 Crypto Crime Trends : Illicit Cryptocurrency Volumes Reach All-Time Highs Amid Surge in Sanctions Designations and Hacking [Ressource électronique] // Chainalysis. - Mode d'accès : <https://www.chainalysis.com/blog/2023-crypto-crime-report-introduction/> (date de référence : 20/02/2024)

⁵ Qu'est-ce que Dusting Attack [Ressource électronique] // Habr. - Mode d'accès : <https://habr.com/ru/articles/450430/> (date de référence : 20/02/2024)

⁶ Dust Attacks Make a Mess in Bitcoin Wallets, but There Could Be a Fix [Ressource électronique] // CoinDesk. - Mode d'accès : <https://www.coindesk.com/tech/2020/08/18/dust-attacks-make-a-mess-in-bitcoin-wallets-but-there-could-be-a-fix/> (date de référence : 20.02.2024)

► **Schéma de blanchiment des ETH volés et de leur conversion pour d'autres jetons (tokens) afin de les échanger contre des BTC**

Source : TRM Labs



de dépôt et de retrait de crypto-monnaie. Grâce à eux, il est possible de suivre les mouvements des actifs virtuels et, dans certains cas, d'identifier le propriétaire des crypto-monnaies.

Les fournisseurs AML ont également recours à l'analyse OSINT. Cela signifie généralement que les experts examinent les données⁷ disponibles publiquement sur des sites tels que YouTube, Telegram, X (ex. Twitter), Reddit, forums, darknet et d'autres plates-formes similaires.

Si seules les adresses des portefeuilles sont connues, les fournisseurs LBC peuvent utiliser les données des transactions passées pour identifier les contacts possibles des suspects avec les services centralisés, qui vérifient souvent leurs clients.

Certains fournisseurs LBC collaborent aussi avec les forces de l'ordre et les bourses de crypto-monnaies, ce qui augmente la possibilité et la rapidité d'identification des malfaiteurs.

Les mixeurs de crypto-monnaie et les « ponts » décentralisés gagnent en popularité afin de rendre plus difficile la traçabilité de la source et du destinataire final. Le tristement célèbre mixeur Tornado Cash a été créé à d'autres fins, mais il a gagné en popularité grâce aux acteurs illégaux du marché des crypto-monnaies.

LES AVANTAGES ET LES INCONVÉNIENTS DES FOURNISSEURS LBC, VOIES DE DÉVELOPPEMENT

Malgré l'amélioration constante des algorithmes, les fournisseurs LBC ont

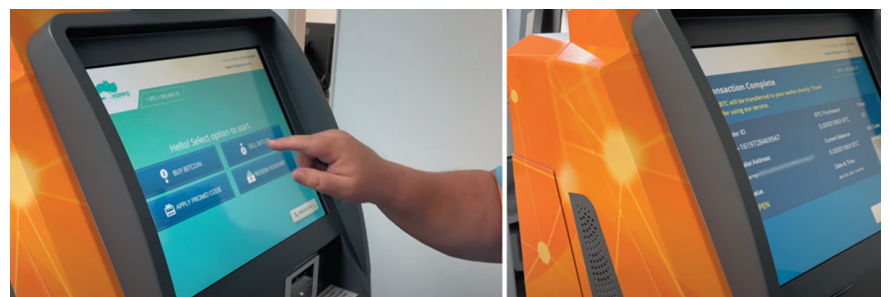
toujours des problèmes. Par exemple, souvent, les fournisseurs ne peuvent pas obtenir de réponses de la part des bourses de crypto-monnaie.

Les différences significatives des exigences des documents réglementaires entre les juridictions rendent beaucoup plus difficile pour les fournisseurs LBC de travailler à l'échelle internationale.

Par exemple⁸, une célèbre bourse centralisée de crypto-monnaie a reconnu publiquement que son utilisateur était engagé dans une fraude importante. Cependant, la plate-forme n'a pas bloqué son client, faisant référence à l'absence de demande de la part des forces de l'ordre.

En outre, chaque grand fournisseur LBC applique ses propres techniques fermés d'analyse des données et de marquage des adresses. D'une part, cela stimule la concurrence sur le marché et aide à résoudre les crimes. D'autre part, l'absence de standards rigoureux entraîne des variations importantes dans la qualité du travail effectué, ainsi que dans la capacité à manipuler les données et le marquage.

Ainsi, en 2021, le GAFI s'est adressé⁹ à un groupe de fournisseurs LBC pour déterminer l'interaction des adresses directement avec les



► **Identification de l'adresse de crypto-monnaie au réseau de machines Bitcoin**

Source : Chainalysis

⁷ The Data Accuracy Flywheel: How Chainalysis Consistently Identifies and Verifies Blockchain Entities [Ressource électronique] // Chainalysis. - Mode d'accès : <https://www.chainalysis.com/blog/chainalysis-data-accuracy/> (date de référence : 20.02.2024)

⁸ KuCoin confirms an exchange user is behind alleged daily rug pulls [Ressource électronique] // Cointelegraph. - Mode d'accès : <https://cointelegraph.com/news/kucoin-meme-coin-daily-rug-pull-confirmation> (date de référence : 20/02/2024)

⁹ Second 12-Month Review Revised FATF Standards Virtual Assets VASPS [Ressource électronique] // FATF. - Mode d'accès : <https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Second-12-Month-Review-Revised-FATF-Standards-Virtual-Assets-VASPS.pdf> (date de référence : 20/02/2024)

bourses et en dehors. La différence entre les informations récapitulatives était si importante que le GAFI a dû reconnaître qu'il n'était pas possible de tirer de bonnes conclusions des résultats.

Grâce à l'élaboration d'une base unifiée d'exigences et à la certification de la qualité des services fournis, les prestataires LBC ont réussi à améliorer leur travail et à garantir la sécurité globale des crypto-monnaies.

En même temps, la réglementation insuffisante constitue un autre problème principal dans ce domaine. De multiples juridictions ont des approches différentes à la réglementation des crypto-monnaies, ce qui pose des problèmes aux fournisseurs LBC des différentes régions. Cela aussi complique la coopération internationale dans la lutte contre la criminalité financière.

Afin de lutter d'une manière efficace contre la criminalité financière dans le domaine des crypto-monnaies, il est nécessaire d'élaborer des normes internationales AML concertées pour la réglementation du marché des crypto-monnaies. Par exemple, le GAFI essaye depuis longtemps d'adapter la réglementation internationale sous des normes communes. Toutefois, on n'a pas réussi à atteindre cet objectif jusqu'à présent.

Les organismes publics devraient coopérer davantage avec les fournisseurs LBC, car cela permet non seulement de réduire le temps nécessaire à la formation du nouveau personnel, mais aussi d'améliorer la qualité des mesures prises.

Il est également important de former les spécialistes dans le domaine de LBC afin qu'ils puissent lutter d'une manière efficace contre la criminalité financière dans le domaine de la crypto-monnaie. Les programmes de formation continue et les cours de certification aideront les spécialistes à développer les aptitudes et les compétences nécessaires.

Par ailleurs, nous aimerions souligner la contradiction des données présentées par un certain nombre de fournisseurs LBC, souvent pour des raisons politiques ou de sanctions. Par exemple, un fournisseur LBC aux États-Unis peut considérer que tel ou tel portefeuille est visé par les sanctions, alors qu'un fournisseur en Fédération de Russie peut avoir des données inverses. Si des actifs provenant d'une telle adresse se retrouvent sur une bourse centralisée légale, par exemple, il pourrait y avoir des divergences, pouvant aller jusqu'au blocage des fonds.

CONCLUSIONS

À la fin de 2023, le volume de la crypto-monnaie « sale » obtenue à la suite d'activités illégales est tombé à 24,2 milliards de dollars contre 39,6 milliards de dollars en 2022.

Le chiffre est toujours élevé, mais il semble dérisoire¹⁰ par rapport à la criminalité dans les marchés financiers traditionnels. Cependant, une approche globale est évidemment nécessaire pour résoudre les crimes dans l'industrie Web3. Dans le même temps, il convient de rappeler qu'il ne s'agit que des « adresses noires » connues, mais il est difficile d'imaginer combien de transactions de crypto-

monnaie sont dans la zone grise, quelle quantité de fonds est potentiellement une violation des politiques LBC des banques et combien d'actifs sont cachés de l'imposition fiscale et de l'identification, donc le chiffre peut être beaucoup plus considérable.

Il est clair que l'élaboration de mécanismes LBC efficaces ne suffira pas à résoudre le problème. Il faut mettre en place une coopération internationale. Il est tout aussi important d'améliorer les compétences des acteurs du secteur des crypto-monnaies en LBC.

Néanmoins, le rôle des fournisseurs LBC dans la lutte contre la criminalité liée aux crypto-monnaies ne doit pas être sous-estimé. C'est grâce à eux que l'industrie de la crypto-monnaie n'est pas enlisée dans les interdictions réglementaires.

L'équilibre entre la sécurité et les données privées est un élément clé d'une réglementation efficace. Les mesures réglementaires LBC ne doivent pas léser les droits des utilisateurs tout en respectant les principes de confidentialité et de sécurité des données.

Le chemin vers un avenir sûr des crypto-monnaies est épineux mais accessible. L'amélioration de la technologie, le développement de la coopération internationale et la cohérence des efforts des gouvernements, des régulateurs, des fournisseurs LBC et des sociétés de crypto-monnaie peuvent créer une base sûre et transparente pour le développement de l'industrie de la crypto-monnaie.

¹⁰ 2023 Fraud and Financial Crime Report [Ressource électronique] / / Kroll. - Mode d'accès : <https://www.kroll.com/en/insights/publications/fraud-and-financial-crime-report> (date de référence : 20/02/2024)



TRAVAIL AVEC LES ACTIFS NUMÉRIQUES : CRYPTOMONNAIE, NFT ET SÉCURITÉ FINANCIÈRE

La révolution numérique marquée par l'émergence de la technologie blockchain et de la cryptomonnaie, représente une nouvelle étape dans l'industrie financière. Elle offre de nouvelles perspectives et lance de nouveaux défis



SEAN MOUNIR,
Directeur général et cofondateur
de la société Coinweb.com

Il est essentiel de comprendre la double nature des actifs numériques : le développement d'innovations et de nouvelles possibilités offertes peuvent également servir aux malfaiteurs dans leurs activités illicites, en particulier dans le cadre de financement du terrorisme.

Vous aurez une idée sur des actifs virtuels et des pratiques qui peuvent changer les activités de votre organisation.

ÉTAT ACTUEL DES CRYPTO-ACTIFS

Nous assistons au 4^e cycle de développement des crypto-monnaies. Bien que ce processus semble chaotique de l'extérieur, il est régularisé et lié à la capitalisation boursière, à l'interaction avec les développeurs, les startups et les médias sociaux.

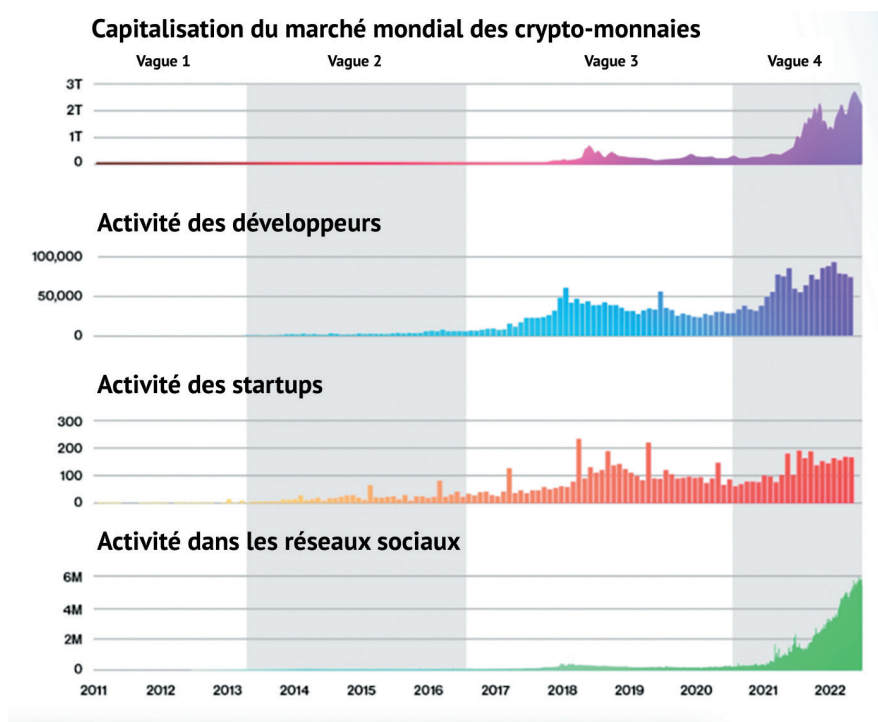
Un ETF bitcoin a été approuvé en 2024 et la même chose se produira avec le Ethereum-ETF. Par ailleurs, la réduction

du bitcoin devrait se produire en mai 2024, ce qui provoquera ensuite une flambée des prix des cryptomonnaies (la période de Bullrun).

Alors que la finance décentralisée (DeFi) était pratiquement inexistante, elle est aujourd'hui estimée à 100 milliards de dollars. Cela a pris deux ans (2020-2022).

Les stablecoins (crypto-monnaie stable) conçus pour assurer la stabilité, comme le dollar des États-Unis ou l'or, sont devenus très répandus dans les régions exposées à l'inflation et la volatilité élevées des devises (en particulier en Afrique, au Proche-Orient et en Asie du Sud-Est).

Dans le même temps, le marché des NFT connaît une croissance explosive, avec des transactions de 44,2 milliards de dollars en 2021, contre 106 millions de dollars l'année précédente. Cependant, ce marché a des problèmes, y compris le Wash Trading et le blanchiment de capitaux.



LUTTE CONTRE LE BLANCHIMENT DE CAPITAUX ET LE FINANCEMENT DU TERRORISME

La crypto-monnaie qui est souvent traité avec scepticisme, est paradoxalement devenue la première industrie à proposer une solution viable au problème du blanchiment de capitaux.

Le progrès réalisé est dus en grande partie à l'évolution rapide de la réglementation et au rôle phare du GAFI, la principale organisation internationale de la lutte contre le blanchiment de capitaux et le financement du terrorisme.

Des mesures doivent être prises d'urgence pour lutter contre le blanchiment de produits de crime et le financement du terrorisme (LBC/FT). Les criminels et les terroristes n'attendent pas l'évolution de la réglementation.

Le secteur privé doit être réglementé

Il faut noter que la demande de réglementation est évidente du

côté du secteur de la crypto. Cela est dû à l'effet de réseau sur les marchés financiers: les organisations préfèrent interagir avec des partenaires soumis à la réglementation pour minimiser ses risques.

Cette demande de réglementation a conduit au développement de solutions réglementaires compétitives qui permettent aux petites sociétés de trading de crypto-monnaies de collaborer avec les acteurs traditionnels du marché financier pour obtenir de l'argent liquide.

Malgré le succès, la capitalisation du marché de la crypto-monnaie est assez modeste, s'élevant à 2 billions de dollars par rapport au volume quotidien de transactions en dollars américains de 2,6 billions.

Coopération entre le secteur privé et les régulateurs

Pour lutter contre la délinquance financière il faut faire des efforts concertés afin de tracer les fonds. Les institutions financières jouent un

rôle primordial dans cet écosystème. Elles sont chargés d'analyser les activités des clients, d'identifier les non-conformités et de suivre les transactions.

Les activités suspectes sont signalées à la Cellule de renseignement financier (CRF), ce qui met l'accent sur les efforts concertés du secteur privé et des régulateurs pour détecter et éliminer la délinquance financière.

NFT COMME NOUVEAU MOYEN DE TOKENISATION DES ACTIFS

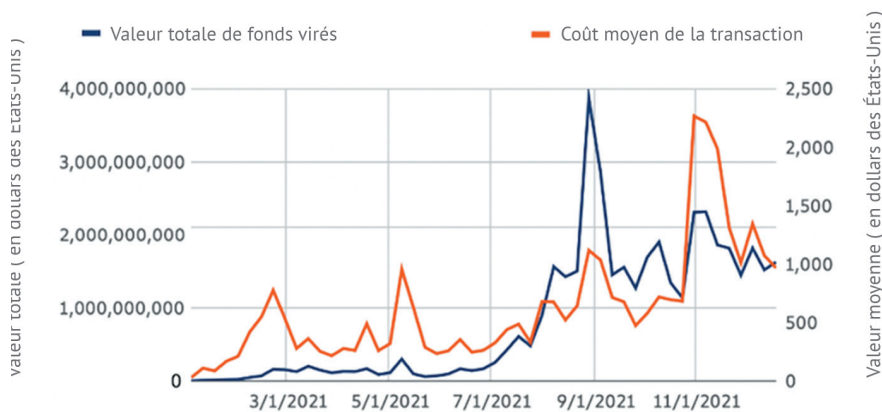
Les jetons non fongibles (NFT) ont révolutionné notre conception de la propriété numérique en transformant les données digitales en actifs uniques sur blockchain.

Cela a commencé avec CryptoPunks en 2017, une collection de 10 000 images pixélisées uniques. Elle a inspiré la création de la norme ERC-721, la base du NFT et des artistes crypto.

NFT et les crimes

Les nouvelles technologies entraînent de nouveaux risques, et NFT n'y fait pas l'exception. La montée en popularité du NFT, en particulier pendant la pandémie COVID-19, a mis l'accent sur la nécessité de créer des plateformes sécurisées et de mettre en œuvre des contrôles de la part des régulateurs.

La pandémie et la baisse des ventes d'objets d'art traditionnels ont détourné les flux d'investissement vers le NFT: le chiffre d'affaires est passé de 106 millions de dollars en 2020 à plus de 17 milliards de dollars en 2021.



Lors de la vérification de son portefeuille, une opération de donation au détenteur anonyme de la crypto-monnaie de collection « Rare Pepe » basée sur Bitcoin a été révélée.

L'utilisation du NFT « Rare Pepe » met l'accent sur le potentiel du NFT dans le financement des activités extrémistes.

FINANCEMENT DU TERRORISME ET LES ACTIFS VIRTUELS

Les organisations terroristes utilisent la crypto-monnaie pour leur financement.

En particulier, en 2020 Al-Qaïda a collecté de l'argent sur des médias sociaux. Grâce aux efforts concertés des forces de l'ordre, plus de 1 million de dollars ont été saisis.

Majoritairement les efforts déployés pour suivre et identifier ces transactions ont abouti, empêchant la légalisation des fonds via des bourses.

NFT propageant des appels au terrorisme

Par exemple, le 6 septembre 2022, l'organisation terroriste l'État Islamique (EI), à l'aide du NFT, a

diffusé un message de soutien à l'attentat en Afghanistan, réalisé par l'État Islamique de la province du Khorassan, une cellule de l'EI en Afghanistan.

C'était la première fois que le NFT était utilisé à des fins terroristes. Un certain nombre d'autres NFT ont été créés par les mêmes acteurs pour explorer les possibilités de contourner les forces de l'ordre et les moyen de modération du contenu de NFT sur différentes plateformes.

NFT et financement de l'extrême droite

Le NFT « Rare Pepe » créé à l'origine comme un même Internet, a commencé à être utilisé par l'extrême droite. Une histoire pareille a eu lieu au mois de décembre 2020 : plus de 500 000 dollars en Bitcoins ont été donnés au représentant de l'extrême droite.

CONCLUSIONS :

L'importance des faits décrits ci-dessus réside dans la possibilité d'utiliser le NFT pour financer le terrorisme. Ils montrent que divers groupes, tels que l'État Islamique, explorent peut-être des options pour collecter des fonds et diffuser des messages à l'aide de nouvelles technologies y compris le NFT.

L'utilisation de NFT par les terroristes pour créer une chaîne de valeur et de financement n'a rien de nouveau. La transmission de NFT « Pepe the Frog » et le développement d'IS-NEWS #01 semblaient inévitables.

Bien que ces NFT n'aient pas été mis en vente, ils restent dans les chaînes de blockchain et sont distribués sur d'innombrables systèmes Internet. Ils sont pratiquement invulnérables aux mesures prises par le Ministère de la Justice ou les forces de l'ordre.

Ainsi, ils résistent à la censure autant que possible, ce qui pose un problème majeur dans la lutte contre le contenu extrémiste.



Rare Pepe PEPEPARADO Créé le 20 septembre 2016 Date de la dernière transaction : le 31 décembre 2021			
Dernier prix 0.08000000	Monnaie XCP	Propriétaires 472	Transactions 145
Offre 4,100,109	Brûlé 1,899,891	Émis 6,000,000	Divisible No
Auteurs + CLAIM	Format JPG		
Open Orders		Trade History	

* Organisation terroriste interdite en Fédération de Russie.

LA NÉCESSITÉ D'UNE RÉGLEMENTATION JURIDIQUE DES PRESTATAIRES DE SERVICES D'ACTIFS VIRTUELS À DES FINS DE LBC/FT DANS TOUS LES PAYS DU MONDE

En octobre 2018, les normes du GAFI ont été appliquées aux activités financières liées aux actifs virtuels. Les recommandations du GAFI sont mises à jour chaque année depuis 2021. En 2020, le rapport du GAFI sur les indices de blanchiment de capitaux et de financement du terrorisme dans la circulation des actifs virtuels, ainsi que le rapport du GAFI aux ministères des finances et aux banques centrales des pays du G20 concernant la cryptomonnaie stable ont été publiés



SOFIA ROUDKOVITCH,
étudiante en 1ère année à l'Université d'État Lomonossov de Moscou, double vainqueur de l'Olympiade internationale sur la sécurité financière (en 2021 et 2022)

Cependant, les PSAV ne sont toujours pas réglementés dans de nombreux pays du monde. Cette lacune rend l'utilisation des actifs virtuels et les PSAV vulnérables aux abus¹, cela crée des obstacles aux enquêtes préliminaires sur les infractions commises à l'aide d'actifs virtuels (par exemple, financement du terrorisme, blanchiment de capitaux) et des difficultés dans la saisie, le blocage et la confiscation d'actifs virtuels d'origine criminelle ou destinés au financement du terrorisme.

Le terme « PSAV » est défini dans le Guide d'application de l'approche fondée sur les risques pour les actifs virtuels et les PSAV. Il s'agit de toute personne physique ou morale qui exerce une ou plusieurs activités commerciales ou opérations pour/ ou au nom d'une autre personne

physique ou morale de:

- 1) l'échange d'actifs virtuels contre de la monnaie fiduciaire et vice versa ;
- 2) l'échange d'une ou plusieurs formes d'actifs virtuels contre d'autres actifs virtuels ;
- 3) virement d'actifs virtuels ;
- 4) la conservation et/ou gestion d'actifs virtuels ou d'instruments permettant de contrôler les actifs virtuels ;
- 5) la participation à la fourniture des services liés à l'offre et/ou à la vente des actifs virtuels de l'émetteur².

Conformément au paragraphe 7 de la Résolution n° 1617 du Conseil de sécurité des Nations Unies du 29 juillet 2005, les Recommandations du GAFI sont obligatoires³. Cependant, en 2022, le GAFI a conclu que seulement une petite partie des États membres avaient suivi les nouvelles Recommandations relatives aux PSAV⁴.

¹ FATF (2022), Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs, FATF, Paris, France : <https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Targeted-Update-Implementation-FATF%20Standards-Virtual%20Assets-VASPs.pdf.coredownload.pdf>, p. 3.

² FATF (2021), Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, FATF, Paris : <https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf>, p. 109.

³ Résolution n° 1617 du Conseil de sécurité des Nations unies du 29 juillet 2005 (adoptée à New York le 29/07/2005 lors de la 5244e réunion du Conseil de sécurité des Nations unies) // Système de référence juridique ConsultantPlus.

⁴ FATF (2022), Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs, FATF, Paris, France, p. 7.

**LES AV (ACTIFS VIRTUELS) ET
LES PSAV (FOURNISSEUR DE
SERVICES D'ACTIFS VIRTUELS)
SONT PRINCIPALEMENT
SOUMISES AUX NORMES DU
GAFI DANS LE DOMAINE DE :**

- l'approche fondée sur les risques des activités et opérations liées aux actifs virtuels et à les PSAV ;
- la surveillance ou le contrôle des PSAV aux fins de LCB/FT ;
- la délivrance de licence ou enregistrement ;
- les mesures de prévention, y compris la vérification des clients, la conservation des dossiers et des documents et la déclaration des transactions suspectes ;
- l'application de sanctions et d'autres pratiques d'application de la loi ;
- la coopération internationale

L'irrégularité du fonctionnement des PSAV n'empêche pas leur travail, mais ne fait qu'augmenter la part du secteur parallèle de l'économie. Une quantité importante de bourses et des bureaux de change de crypto-monnaies travaillent hors du cadre légal, ils ne sont enregistrés dans aucune juridiction, n'identifient pas les propriétaires d'adresses Bitcoin, n'effectuent pas de procédures de conformité et ne respectent aucune exigence. Cela permet d'utiliser des crypto-monnaies pour commettre des crimes, y compris le blanchiment de capitaux et le financement du terrorisme en restant impuni⁵.

L'absence de réglementation du statut légal des PSAV s'aggrave considérablement dans le cadre du procès pénal. La saisie des revenus

de la criminalité sous forme de crypto-monnaie s'effectue de deux manières :

- 1) dans le cadre d'investigations ou d'enquêtes, en saisissant des portefeuilles de crypto-monnaie « froids » (matériels) ou en obtenant la clé privée du propriétaire du portefeuille de crypto-monnaie, ce qui permet aux agents de forces de l'ordre d'avoir accès aux revenus des criminels ;
- 2) par l'interaction avec les PSAV.

Si, au cours d'enquête ou d'investigation, on ne réussit pas à saisir un portefeuille de crypto-monnaie ou une clé privée, le seul moyen de saisir ou de bloquer des crypto-monnaies est l'envoi par les forces de l'ordre d'une demande concernant les données suivantes aux PSAV concernés utilisés par le suspect/accusé : nom, prénom, patronyme, détails de la pièce d'identité, nationalité, adresse de résidence, photo de l'utilisateur, informations de contact, adresse IP, détails de l'utilisation du VPN, adresse IP réelle lors de l'utilisation d'un logiciel d'anonymisation des adresses, géolocalisation, détails de l'appareil du client, statistiques, préférences, activités, numéro de compte du bénéficiaire, date et heure de l'ouverture du compte, statut de la transaction d'échange, montant du dépôt et du retrait⁶. Cette méthode n'est appropriée que si le PSAV exerce légalement ses activités et effectue la vérification de ses utilisateurs conformément aux principes KYC (Know Your Client), par exemple, avec la présentation obligatoire d'une copie du passeport, une photo avec un passeport à la main lors de l'enregistrement⁷.

Ces informations sont souvent proposées par les prestataires de services d'actifs virtuels sur la base

du droit national. Toutefois, en réalité, cette règle pour les PSAV n'est qu'une « confiance mutuelle » : les PSAV situés dans des juridictions étrangères négligent leurs obligations de donner des informations sur leurs clients et évitent de le faire. Malgré cela, dans certains pays où la réglementation juridique des activités des PSAV est en cours d'élaboration, il existe une pratique consistant à fournir des informations des PSAV enregistrées dans d'autres États⁸.

Compte tenu des risques élevés que comporte l'absence de réglementation du statut juridique des PSAV, je considère nécessaire ce qui suit :

- 1) effectuer une classification généralisée des PSAV dans tous les pays du monde en tant que entités LCB/FT, enregistrement et délivrance des licences ;
- 2) fixer un seuil de transactions occasionnelles, au-delà duquel les PSAV sont obligés de prendre des mesures appropriées de vigilance à l'égard de leur clientèle, par exemple, les lignes directrices du GAFI fixent 1 000 dollars américains/euros.

Les lignes directrices du GAFI du 2021 soulignent l'importance de la coopération internationale entre les autorités de surveillance, compte tenu de la nature transfrontière des activités et des services de PSAV. Il est certain que dans la situation actuelle où les risques d'utilisation d'actifs virtuels à des fins criminelles ne cessent de croître, les États doivent s'unir dans la lutte contre les nouveaux défis et menaces et ne pas politiser le domaine de la coopération dans la lutte contre la criminalité.

⁵ O. N. Tissène. Identification des propriétaires de portefeuilles de crypto-monnaie, détection et saisie des clés privées dans les enquêtes de procédure pénale // Procès pénal. 2024. N° 1. P. 78-83.

⁶ FATF (2021), Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, FATF, Paris, p. 80.

⁷ O. N. Tissène. Techniques de détection et d'investigation des crimes commis avec des crypto-monnaies. Moscou, 2023. P. 53.

⁸ O. N. Tissène. Suivi des transactions de crypto-monnaie pour mener une enquête criminelle // Procès pénal. 2024. N° 2. P. 54-59, P. 59.

Je suis la lauréate de première et deuxième Olympiades internationales sur la sécurité financière. Lorsque j'étais en seconde, j'ai découvert les Olympiades dans les réseaux sociaux et j'ai eu immédiatement envie d'y participer. Depuis la troisième, je m'intéressais au droit et j'étais membre de l'équipe de droit de Moscou. J'ai étudié les normes du GAFI et la législation russe en matière de LBC/FT, ainsi que des vidéos sur la sécurité financière pour me préparer à l'Olympiade. Comme je me suis bien préparée, j'ai réussi à me qualifier pour la finale et à gagner.



Le programme de la finale de l'Olympiade internationale sur la sécurité financière m'a frappé, m'a incité à faire mieux et m'a aidé à choisir mon futur métier. J'aime surtout le programme de la finale de l'Olympiade. L'étape finale prend environ une semaine, mais il ne reste que deux heures pour accomplir les tâches. Le reste du temps est consacré à des excursions, des divertissements et des activités de formation, au cours desquelles nous avons suivi le cours théorique et pratique de LBC/FT.

marquant pour moi et mes amis nous permettant non seulement d'améliorer nos connaissances, mais aussi de montrer notre créativité, talent d'acteur et nos compétences de communication.

Je me souviendrai toujours de ma rencontre avec Youri Anatolievitch Tchikhantchine, directeur de Rosfinmonitoring, un grand homme et un vrai professionnel.

L'histoire de la lutte de notre pays contre les crimes financiers m'émerveille et m'inspire. En 2001, notre pays a été mis au défi : on nous a inscrit sur la liste noire du GAFI. Grâce aux efforts conjoints, la Fédération de Russie est aujourd'hui, après 20 ans, un État doté de l'un des systèmes les plus efficaces de lutte contre la criminalité financière.

À l'avenir, j'aimerais me consacrer à la sécurité financière et devenir une chercheuse dans ce domaine et appliquer mes connaissances.



L'organisation de la finale de l'Olympiade internationale sur la sécurité financière est très différente de celle des autres Olympiades de la liste, y compris l'Olympiade panrusse des écoliers où j'ai remporté la victoire à plusieurs reprises en 2020-2022.

Méthodologie inoubliable des activités de formation du programme de l'Olympiade finale. Le procès pénal sous forme de jeu inspiré par le film soviétique « La main de diamant », la quête « Blanchiment de capitaux sur la base des dessins animés et des films » ont été un événement



ACTUALITÉS DU SYSTÈME ANTI-BLANCHIMENT

-
- 84** « Jeux de l'avenir ». Les gagnants du tournoi « la coupe des quatre continents » ont visité kazan
-
- 85** La tenue de la première réunion en format élargi du Conseil des BRICS sur la lutte contre le blanchiment de capitaux et le financement du terrorisme
-
- 85** Les problèmes de sécurité financière ont été discuté au Festival mondial de la jeunesse
-

« JEUX DE L'AVENIR ». LES GAGNANTS DU TOURNOI « LA COUPE DES QUATRE CONTINENTS » ONT VISITÉ KAZAN

Les finalistes de la IIIe Olympiade internationale sur la sécurité financière, les jeunes de Russie, d'Algérie, d'Iran, de Cuba, du Kirghizistan, d'Ouzbékistan et du Tadjikistan se sont retrouvés dans la capitale du Tatarstan pour les « Jeux de l'avenir »

Lors de la finale de l'Olympiade, les jeunes ont montré leur meilleure performance dans le tournoi de football figital. Ils ont fait connaissance avec d'autres type de cybersport à Kazan. Les étudiants avaient été invités aux compétitions internationales multisports « Jeux de l'avenir » par Dmitri Tchernychenko, le vice-président du Gouvernement de la Fédération de Russie. Jordan Antonio Rodríguez, de nationalité cubaine, un des invités et participant à l'Olympiade, a fait connaissance à distance avec la Russie dès son enfance : sa grand-mère a déménagé à Cuba quand elle était jeune, mais n'a jamais oublié sa Patrie. Le jeune homme a écouté des histoires sur notre pays, et en 2023 il est venu à Sirius pour participer à l'Olympiade internationale sur la sécurité financière. Nous avons demandé à Antonio de partager ses idées sur l'avenir de la sécurité financière internationale : « Les gens et les gouvernements doivent prendre conscience de son importance dans le monde hautement globalisé et technologique d'aujourd'hui : pour la protection de leurs fonds personnels et pour la sécurité de leurs pays. Je rêve d'une coopération globale en matière de sécurité financière, où les divergences politiques et économiques sont mises de côté et où l'on s'unit pour éradiquer le terrorisme et des choses comme le blanchiment de

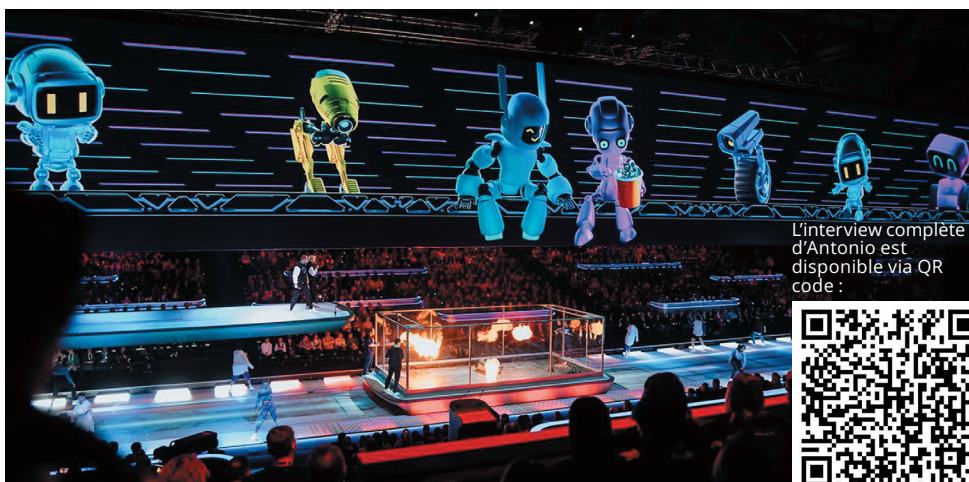
capitaux. Mais pour l'instant, il s'agit encore d'une utopie ».

Deux participants, Fateh Bousri d'Algérie et Bahriddin Roustamov du Tadjikistan ont continué leur voyage en Russie et ont assisté au Festival mondial de la jeunesse dans le territoire fédéral de Sirius. En prenant part au riche programme du Festival, ces jeunes ont trouvé du temps pour partager leurs impressions sur les « Jeux de l'avenir » et l'Olympiade internationale sur la sécurité financière. « J'étais capitaine de l'équipe internationale « Les loups » qui a gagné le match de football figital à l'Olympiade sur la sécurité financière l'année précédente. C'est pourquoi nous avons été invités à Kazan pour les « Jeux de l'avenir », et maintenant je suis au Festival mondial de la jeunesse. Je veux non seulement développer mes connaissances en matière de sécurité financière, mais aussi les partager. Je me prépare activement à la prochaine Olympiade, je veux vraiment aller



en finale. En outre, je participe à des activités d'enseignement au sein du Mouvement, en essayant de parler du projet dans mon pays », a déclaré Bahriddin.

Parmi les impressions les plus vives de Fateh figurent les rencontres avec des politiciens et des athlètes célèbres du monde entier : « Une impression inoubliable lors de ma participation aux « Jeux de l'avenir » est ma rencontre avec Vladimir Poutine, le président de la Fédération de Russie, pendant la cérémonie d'ouverture ainsi que la possibilité d'assister à l'événement depuis la loge des invités d'honneur avec les chefs d'État. C'était un grand honneur pour moi et j'en garde de beaux souvenirs. Je tiens à vous remercier tous pour votre hospitalité, et j'ai bien sûr l'intention de visiter à nouveau la Russie. »



L'interview complète d'Antonio est disponible via QR code :



LA TENUE DE LA PREMIÈRE RÉUNION EN FORMAT ÉLARGI DU CONSEIL DES BRICS SUR LA LUTTE CONTRE LE BLANCHIMENT DE CAPITAUX ET LE FINANCEMENT DU TERRORISME

Rosfinmonitoring (Service fédéral de surveillance financière) a organisé la première réunion en vidéoconférence du Conseil des BRICS sur LBC/FT en 2024

Les participants à la réunion ont discuté du développement des systèmes nationaux de lutte contre le blanchiment de capitaux et de nouvelles mesures conjointes visant à garantir la sécurité financière.

Dans le cadre de la présidence russe des BRICS des initiatives visant



à améliorer la transparence des systèmes financiers, à minimiser les risques et les menaces, à renforcer la collaboration entre l'État et le secteur privé et à impliquer les jeunes dans le domaine de la sécurité financière ont été présentées. En particulier, des projets tels que le Centre international

d'évaluation des risques, le service « Blockchain transparente », l'Olympiade internationale sur la sécurité financière et le Conseil international de la conformité ont suscité l'intérêt.

Les parties se sont déclarées convaincues que le Conseil des BRICS sur LBC/FT peut fournir une contribution importante au système mondial de la lutte contre le blanchiment de capitaux et le financement du terrorisme, ainsi qu'à la mise en œuvre de la Stratégie de partenariat économique des BRICS jusqu'à 2025.

LES PROBLÈMES DE SÉCURITÉ FINANCIÈRE ONT ÉTÉ DISCUTÉ AU FESTIVAL MONDIAL DE LA JEUNESSE

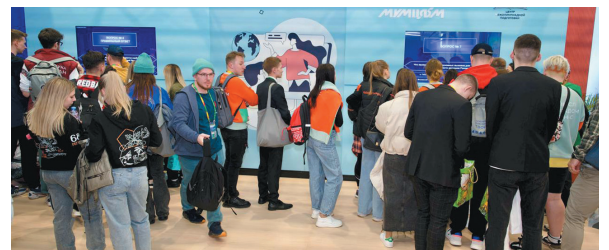
En mars, des jeunes du monde entier se sont réunis dans le cadre d'un événement exceptionnel à Sirius

Le Festival mondial de la jeunesse a accueilli 20 000 leaders russes et étrangers du monde des affaires, des médias, de la coopération internationale, de la culture, de la science, de l'éducation, du bénévolat, de la charité, du sport et de divers domaines de la vie publique, ainsi que des adolescents représentant diverses organisations et associations pour les enfants.

Les problèmes de sécurité financière ont également fait une partie

importante de l'agenda du Festival. Les experts de Rosfinmonitoring (Service fédéral de surveillance financière),

du Centre international de formation et de méthodologie pour la surveillance financière (ITMCFM) et de la PSB (Promsvyazbank) ont présenté le stand de Sodruzhestvo et ont organisé plusieurs activités pour les participants au Festival. Parmi eux il y a eu plus de 50 finalistes de l'Olympiade internationale de la sécurité financière, ainsi que de jeunes agents des cellules de renseignement financier des pays étrangers.



Le Mouvement international des Olympiades de la sécurité financière ainsi que la manière d'y adhérer et les modalités de participation à l'Olympiade de 2024 ont été présentés aux jeunes. Lors de discussions et de jeux d'affaires, les jeunes gens ont abordé des questions d'actualité relatives à la lutte contre la criminalité financière et ont partagé l'expérience de leurs pays.



COMITÉ ÉDITORIAL



**Président du
comité éditorial**
Youri
Tchihantchine



**Vice-président du
comité éditorial**
Vladimir
Ovtchinnikov



**Vice-président du
comité éditorial**
Guerman Neglyade



**Rédacteur
en chef**
Irina Riazanova

MEMBRES DU COMITÉ ÉDITORIAL



Galina Bobrycheva



Ivan Kornev



Oleg Krylov



Anton Lisitsyn



Sergueï Tétéroukov



Alexeï Petrenko



Margarita Andronova

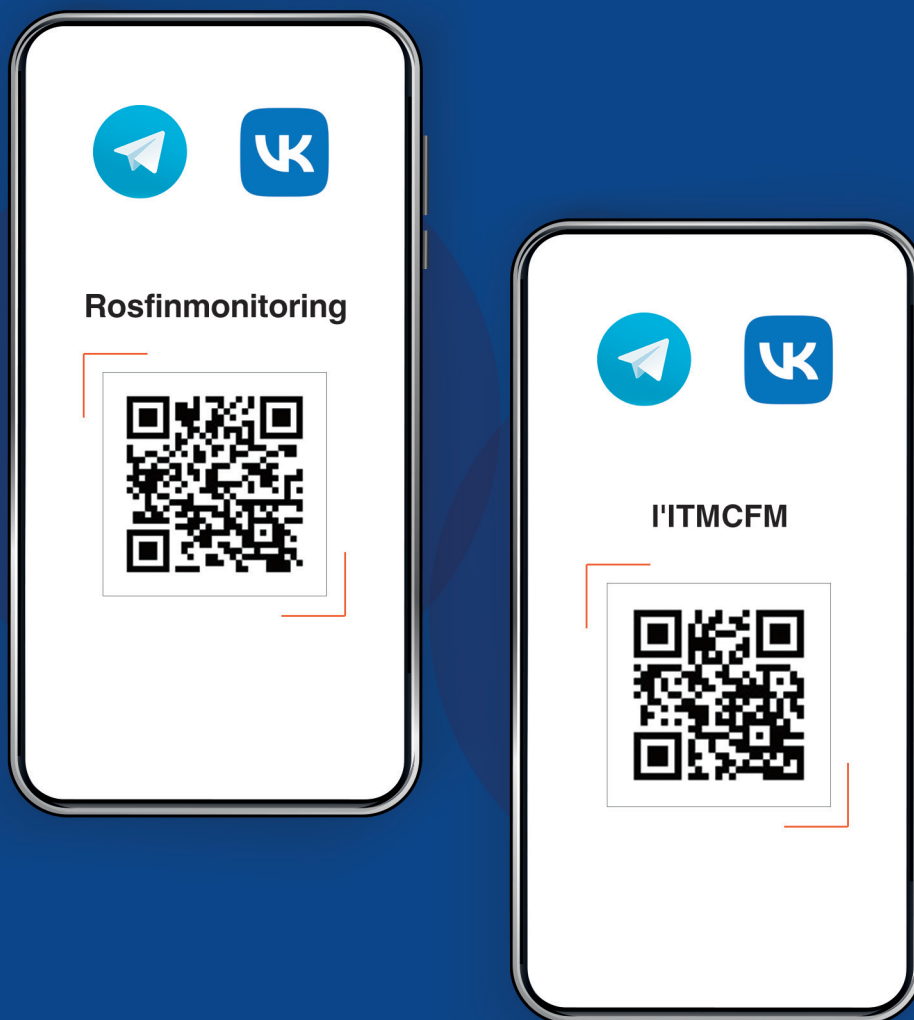


Ievgueni Guileta



Marina Chemiakina

Rosfinmonitoring et l'ITMCFM sur Telegram et VKontakte



Édition

Organisation autonome à but non lucratif
Centre international de formation et de méthodologie pour le suivi financier
31, ruelle Staromonetny, bâtiment 1, 119017 Moscou
E-mail : info@mumcfm.ru
Tirage : 600 exemplaires.

Les opinions des rédacteurs ne coïncident pas nécessairement avec celles des auteurs.

ITMCFM
2024