LA SURVEILLANCE DES MOYENS DE PAIEMENT SCRIPTURAUX ET DES INFRASTRUCTURES DES MARCHÉS FINANCIERS

RAPPORT 2020

BANQUE DE FRANCE
EUROSYSTÈME

LA SURVEILLANCE DES MOYENS DE PAIEMENT SCRIPTURAUX ET DES INFRASTRUCTURES DES MARCHÉS FINANCIERS

RAPPORT 2020

BANQUE DE FRANCE
EUROSYSTÈME

SOMMAIRE

AVANT-PROPOS

En application de l'article L141-4 § I et II du Code monétaire et financier, la Banque de France veille :

• au bon fonctionnement et à la sécurité des systèmes de paiement ;

• à la sécurité des systèmes de compensation, de règlement et de livraison des instruments financiers ;

• à la sécurité des moyens de paiement scripturaux et à la pertinence des normes applicables en la matière.

Le bon fonctionnement et la sécurité des infrastructures des marchés financiers et des moyens de paiement sont essentiels à l'économie dans son ensemble : ils sont nécessaires à la mise en œuvre efficace de la politique monétaire, et contribuent à la stabilité financière et à la confiance des agents économiques dans la monnaie.

De façon régulière, la Banque de France rend compte au public de l'exercice de ses missions de surveillance sur les infrastructures des marchés financiers et sur les moyens de paiement. Le rapport précédent datait de 2017.

Le présent rapport couvre la période allant de 2018 à 2020.

INTRODUCTION

Au cours de ces trois dernières années, la surveillance des infrastructures de marché et des moyens de paiement scripturaux, tout en s'inscrivant dans la continuité de la période précédente, a été marquée par plusieurs évolutions significatives, tenant tant aux modifications apportées au cadre réglementaire qu'à l'émergence de nouveaux défis ou à l'amplification de tendances observées précédemment.

Le cadre réglementaire, profondément rénové durant les années précédentes, avec l'entrée en vigueur de plusieurs textes particulièrement structurants, qu'il s'agisse notamment du règlement EMIR [1] sur les contreparties centrales (CCP), du règlement sur dépositaires centraux de titres (CSDR [2]) ou de la deuxième directive sur les services de paiements (DSP2), a en particulier été précisé au travers de plusieurs standards techniques et complété sur plusieurs points. S'agissant des CCP, ces compléments ont porté, d'une part, sur la surveillance des contreparties centrales issues de pays tiers – l'objectif, dans la perspective du Brexit, ayant été de renforcer les prérogatives des autorités européennes à l'égard des CCP considérées comme systémiques pour l'UE –, d'autre part, sur le cadre applicable en matière de rétablissement et de résolution, de façon à incorporer en droit de l'Union européenne (UE) les principes arrêtés par le Conseil de stabilité financière (*Financial Stability Board*, FSB) en la matière. Au-delà des CCP, l'Eurosystème a par ailleurs, dans le droit-fil des principes afférents aux comités CPMI [3] et IOSCO [4], précisé ses attentes en matière de surveillance du cyberrisque à l'égard des infrastructures de marché de son ressort, dans un contexte caractérisé par la montée des menaces. Dans le domaine des paiements de détail, il s'est avant tout agi de mettre en œuvre la DSP2, entrée en vigueur début 2018, en particulier pour ce qui est de son volet sécuritaire, et notamment dans le cadre de l'Observatoire de la sécurité des moyens de paiement. Enfin, dans le sillage des travaux menés par le G7 en 2019, sous présidence française, puis du FSB, la Commission européenne a, fin 2020, publié une proposition législative sur l'encadrement réglementaire des cryptoactifs, dans le cadre d'un ensemble de textes sur la finance numérique ; la phase de négociations qui a été initiée permettra d'affiner autant que de besoin le contenu des mesures proposées, mais il s'agit en toute hypothèse d'une évolution majeure, à même de permettre à l'UE de répondre aux défis des nouvelles technologies.

Les actions de surveillance menées par la Banque de France se sont quant à elles concentrées autour de trois grands axes. Le premier a été – et reste – l'évaluation récurrente de la conformité des infrastructures de marché aux textes auxquels celles-ci sont soumises, les analyses conduites dans ce cadre permettant de passer en revue l'ensemble des risques auxquels elles sont exposées (financiers, opérationnels, cyber, etc.), tout comme les mécanismes en place ou les mesures prises pour les prévenir, et *in fine* de s'assurer tant de leur robustesse que de leur performance. Le second, dans le domaine des moyens de paiement scripturaux, a porté sur un ensemble d'actions visant à renforcer la sécurité de ces derniers, qu'il s'agisse notamment de l'accompagnement de la Place – complété par un suivi individuel – pour la mise en œuvre progressive de l'authentification forte du client, ou de l'analyse des dispositions sécuritaires prises par les émetteurs de moyens de paiement. Un troisième axe a été, en 2020, le suivi renforcé tant des infrastructures de marché que des acteurs de la chaîne des paiements de détail, pour s'assurer de leur résilience face aux risques notamment opérationnels induits sur leurs systèmes d'information, et de leur organisation à la suite de la pandémie de Covid-19 – et force est de constater qu'ils ont su y faire face.

1 Règlement européen relatif aux infrastructures des marchés financiers – *European Market Infrastructure Regulation.*

2 *Central Securities Depositories Regulation.*

3 Comité sur les paiements et les infrastructures de marché – *Committee on Payments and Market Infrastructures. https://www.bis.org/cpmi/*

4 Organisation internationale des commissions de valeurs – *International Organization of Securities Commission. https://www.iosco.org/*

1

LA SURVEILLANCE DES INFRASTRUCTURES DES MARCHÉS FINANCIERS

LA SURVEILLANCE DES INFRASTRUCTURES DES MARCHÉS FINANCIERS

La Banque de France est impliquée, en tant qu'autorité nationale compétente, dans la surveillance des infrastructures de marché françaises, aux côtés de l'Autorité de contrôle prudentiel et de résolution (ACPR) et de l'Autorité des marchés financiers (AMF), selon les entités concernées. Elle participe également à la surveillance coopérative de plusieurs infrastructures de marché et systèmes de paiement européens et internationaux.

1 Les évolutions réglementaires dans le domaine des infrastructures des marchés financiers

Alors que les deux précédentes périodes (2012-2014 et 2015-2017) avaient été marquées par la transposition en droit communautaire des principes pour les infrastructures des marchés financiers (PFMI), définis en 2012 par les comités CPMI et IOSCO [5], la période sous revue a connu des évolutions reflétant tant la prise en compte de nouveaux enjeux, qu'il s'agisse tout particulièrement des amendements apportés à EMIR, des avancées sur le rétablissement et la résolution des CCP, ou des développements liés à la prévention du cyberrisque.

1.1 Un renforcement du cadre réglementaire CCP combiné à une adaptation des obligations de compensation imposées aux acteurs financiers

Le règlement européen EMIR régissant ces dispositions, publié en juillet 2012, a fait l'objet de deux révisions au cours de la période sous revue, l'une axée sur le volet relatif à l'obligation de compensation et au *reporting*, et ayant eu pour objectif de favoriser une mise en œuvre proportionnée des exigences réglementaires en la matière (dite « EMIR REFIT » pour *Regulatory Fitness*), l'autre, centrée sur le dispositif de surveillance des CCP de pays tiers et des CCP de l'UE (dite « EMIR 2.2 »).

Le premier point a donné lieu à la publication, le 20 mai 2019, du n° 2019/834 (EMIR REFIT) ; ce dernier prévoit des allègements en matière d'obligation de compensation et de *reporting*, notamment pour les contreparties non financières, et de nouvelles exigences applicables aux CCP (avec par exemple l'introduction d'un principe d'accès « juste, raisonnable, non discriminatoire et transparent » à la compensation pour les acteurs financiers).

Le second point, qui s'est traduit par le règlement 2019/2099 du 23 octobre 2019 (dit EMIR 2.2), prévoit la refonte du cadre de supervision des CCP de pays tiers et des CCP de l'UE. Les ambitions du texte étaient, d'une part, de renforcer la maîtrise du risque systémique concentré dans les CCP *offshore*, par l'introduction d'un régime réglementaire et de supervision proportionné, et d'autre part d'harmoniser la supervision des CCP de l'UE par un rôle accru de l'Autorité européenne des marchés financiers (AEMF).

Concernant les CCP établies hors de l'UE, le régime initial, fondé sur l'équivalence des cadres réglementaires, ne permettait pas aux autorités européennes d'exercer un réel contrôle sur ces infrastructures. Pour remédier à cette lacune, potentiellement préjudiciable à la stabilité financière européenne, dans le contexte du Brexit en particulier, la revue EMIR a conduit à mettre en place un dispositif à trois étages (*tier*), aboutissant à un classement des CCP selon leur systémicité pour l'UE :

- CCP de Tier 1 : pour les CCP non systémiques, le dispositif de reconnaissance fondé sur l'équivalence des cadres réglementaires est revu régulièrement et assorti de conditions pour assurer la réalité de l'équivalence ;
- CCP de Tier 2 : pour ces CCP d'importance systémique, la conformité aux standards de l'EMIR est exigée et vérifiée par une supervision directe de l'AEMF, à travers une nouvelle instance dédiée, le CCP Supervisory Committee (ou comité de supervision des CCP, également compétent sur les CCP de l'UE) ;

5 La Banque de France et l'Autorité des marchés financiers sont les membres français du CPMI-IOSCO.

- Au-delà : pour les activités de compensation « d'une importance systémique substantielle », un pouvoir discrétionnaire de refus de reconnaissance est confié à la Commission, sur recommandation de l'AEMF et après accord des banques centrales d'émission concernées (article 25(2c) EMIR). Ce refus de reconnaissance imposera la relocalisation des segments d'activité concernés dans l'UE, pour pouvoir continuer à proposer des services à des entités européennes.

Les actes d'exécution précisant ce dispositif à trois étages, publiés par la Commission en septembre 2020, font apparaître que seules les CCP britanniques LCH Ltd et ICE Clear Europe seront soumises au régime de supervision du Tier 2. En parallèle, les autorités européennes ont insisté sur la nécessité pour les acteurs financiers européens de réduire leurs expositions sur ces CCP d'ici à juin 2022, date de fin de la période d'équivalence temporaire du Royaume-Uni accordée par la Commission européenne. De la même manière, l'AEMF s'est publiquement engagée [6] à conduire à l'horizon du premier semestre 2022 une revue exhaustive de l'importance systémique de ces deux CCP pour l'UE, et le cas échéant à engager une procédure au titre de l'article 25(2c) de EMIR 2.2 (pouvant conduire à la non-reconnaissance totale ou partielle des CCP les plus systémiques).

Concernant les CCP établies dans l'UE, la compétence de supervision reste nationale. Cependant, le rôle de l'AEMF a été renforcé (rédaction de nouvelles orientations et standards techniques, avis *ex ante* obligatoire sur certains projets des CCP), permettant de favoriser une plus grande convergence des approches nationales. Ainsi le CCP Supervisory Committee, établi au début de l'année 2020 et réunissant notamment toutes les autorités compétentes nationales en charge de la supervision de CCP, a déjà acquis un rôle central dans l'harmonisation des pratiques de supervision des CCP européennes, de par son intervention obligatoire dans un certain nombre de dossiers (par exemple pour les modifications de modèles de marge, l'introduction de nouveaux produits, ou le contrôle des fusions-acquisitions).

1.2 Le rétablissement et la résolution des contreparties centrales : un cadre international précisé, un cadre européen quasi finalisé

Un cadre international précisé

Le rétablissement d'une infrastructure de marché concerne toutes les mesures permettant la continuité d'activité et de fourniture des services essentiels de l'infrastructure dans le cas de la survenance de pertes dont l'ampleur dépasserait les mécanismes habituels d'absorption des pertes (en particulier les marges collectées par les CCP et leurs fonds de défaut). Les infrastructures de marché peuvent subir deux grands types de pertes : celles qui sont liées au défaut d'un membre, et celles qui ne le sont pas (fraude interne, fraude externe, pertes sur investissements propres de l'infrastructure, etc.). Le rétablissement incombe aux infrastructures elles-mêmes, qui doivent prévoir ces mesures dans leurs règles internes. La résolution pour sa part est initiée et conduite par les autorités de résolution, notamment lorsque la phase de rétablissement a échoué ou lorsqu'il est nécessaire de l'interrompre pour des raisons de stabilité financière, et vise à permettre la cessation ordonnée de l'activité, en évitant au maximum le recours aux deniers publics [7].

Compte tenu du caractère systémique des CCP, et des enjeux financiers spécifiques associés au rétablissement et à la résolution de telles infrastructures, le FSB a jugé nécessaire d'étendre les dispositifs de rétablissement et de résolution à ce type d'entité, de manière à couvrir tous les scénarios de crise envisageables, même peu plausibles.

Dès fin 2014, le FSB a adopté des recommandations portant sur la résolution des CCP [8]. En complément, il a publié le 5 juillet 2017 [9] une orientation établissant un cadre harmonisé au niveau international, selon laquelle, dans le but d'assurer une résolution ordonnée, les autorités disposeront d'outils et de pouvoirs étendus (pouvoirs de résiliation partielle ou totale des contrats, d'allocation forcée des positions ouvertes ou des pertes, etc.). Pour encadrer l'exercice de ces pouvoirs, l'orientation consacre d'une part le principe d'équité dans le partage des pertes (*pari passu*), distinguant les situations liées au défaut d'un membre compensateur des situations de non-défaut, et d'autre part le principe de traitement non défavorable des créanciers au regard des règles de la liquidation (principe du *no creditor worse off* – NCWO). Les ressources financières revêtent par conséquent une importance particulière pour les autorités qui, afin de mener à bien la résolution (évaluations de résolvabilité), seront amenées à effectuer des évaluations précises des besoins financiers.

L'orientation impose l'adoption de plans de résolution pour toutes les CCP d'importance systémique, sur la base d'une coopération étroite entre les autorités concernées au sein d'une juridiction (entre les autorités de résolution et de supervision) et à l'international (mise en place de *crisis management groups* – CMG).

Ces travaux du FSB se poursuivent depuis 2017, avec la négociation d'une *Guidance* (ligne directrice publiée

le 16 novembre 2020) portant sur deux volets. Il s'agit dans un premier temps, en matière d'adéquation des ressources, de définir une méthodologie en cinq étapes, ayant vocation à être suivie par les autorités de résolution de CCP systémiques, afin d'analyser la nature, la disponibilité et le montant des ressources disponibles au sein de la CCP en cas de résolution ainsi que l'opportunité, en cas de manque de ressources, d'envisager le recours à des ressources additionnelles au moyen de pouvoirs statutaires renforcés.

Dans un deuxième temps, la *Guidance* avait initialement vocation à clarifier le traitement des actionnaires de CCP en résolution. En effet, il existe une tension particulière en la matière pour les CCP : d'une part, les *key attributes* du FSB et la *Guidance* de 2017 entérinent le principe fondamental de la résolution selon lequel les actionnaires doivent absorber les pertes ; d'autre part, les règles contractuelles des CCP prévoient que le capital n'absorbe qu'une partie limitée des pertes (soit le fait pour une CCP d'avoir à exposer une fraction de son capital au risque de pertes - en l'espèce, jusqu'à 25 % de ce dernier en Union européenne). Les négociations n'ont pas permis d'aboutir à un compromis au sein du FSB sur ce sujet, qui pourrait être finalement laissé à la main des autorités de résolution dans chaque juridiction.

Un cadre européen finalisé

Au niveau européen, la Commission européenne a publié fin novembre 2016 un projet de règlement sur le rétablissement et la résolution des CCP. Temporairement suspendue en 2018 dans l'attente de la finalisation de EMIR 2.2 et des travaux internationaux au FSB, la négociation a repris courant 2019 et s'est achevée dans le courant de l'été 2020, avec une publication prévue au *Journal officiel de l'Union européenne* début 2021. Ce texte vise à décliner les standards internationaux dans le cadre juridique de l'Union ; celle-ci reprend donc les principales conclusions des *key attributes* du FSB : i) encadrer les mesures prises par les CCP dans le cadre de leurs plans de rétablissement ; ii) accorder aux autorités de résolution les pouvoirs nécessaires à la résolution d'une CCP non viable ; et iii) définir les outils appropriés de résolution. L'objectif est d'éviter de recourir aux deniers publics, si ce n'est en ultime ressort.

Le texte prévoit globalement une responsabilité accrue des actionnaires, notamment en cas de pertes non liées à un défaut (donc purement attribuables à la gestion de la CCP), sans pour autant exonérer les participants de leur participation aux pertes. Le cadre ainsi défini doit être précisé par des standards techniques réglementaires, qui seront élaborés à partir de 2021.

1.3 La révision du règlement pour les systèmes de paiement d'importance systémique

Une première révision du règlement (UE) n° 795/2014 de la BCE du 3 juillet 2014 (dit règlement SPIS) concernant les exigences de surveillance applicables aux systèmes de paiement d'importance systémique (SPIS) en 2017, a été réalisé à travers le règlement (UE) 2017/2094 de la BCE du 3 novembre 2017. Cette révision a apporté des précisions sur les obligations existantes, a intégré de nouvelles exigences en matière de gestion des risques (notamment en matière de cyberrésilience) et a élargi les pouvoirs des autorités.

Les opérateurs des quatre SPIS avaient alors un délai de douze mois pour se mettre en conformité avec le règlement révisé (dix-huit mois pour les dispositions relatives aux obligations financières). À la suite de l'autoévaluation incombant aux opérateurs, les autorités compétentes (la Banque de France pour CORE(FR), la BCE pour TARGET2, EURO1 et STEP2-T) ont conduit une évaluation d'écart sur la conformité des SPIS aux nouvelles exigences. Cette phase d'évaluation a été conclue en juillet 2020.

En parallèle de la conduite de cette phase d'évaluation, Mastercard CMS a été identifié comme SPIS par le Conseil des gouverneurs le 4 mai 2020. Ce nouveau SPIS sera surveillé par deux autorités compétentes (la BCE et la Banque nationale de Belgique).

Le règlement SPIS fera prochainement l'objet d'une nouvelle révision, afin notamment de préciser les modalités d'une surveillance conjointe par deux autorités compétentes. Cette révision visera également à détailler et à clarifier la procédure permettant de désigner un système de paiement comme SPIS.

6 *https://www.esma.europa.eu/press-news/esma-news/esma-recognise-three-uk-ccps-1-january-2021*

7 *https://www.bis.org/cpmi/publ/d00b.htm ?&selection=156&scope=CPMI&c=a&base=ter*

8 *http://www.fsb.org/wp-content/uploads/r_141015.pdf*

9 *http://www.fsb.org/wp-content/uploads/P050717-1.pdf*

1.4 La réglementation européenne « CSDR » pour l'harmonisation du règlement de titres et le renforcement du cadre d'exercice des dépositaires centraux de titres

Le règlement (UE) 909/2014 visant l'harmonisation, au sein de l'UE, des exigences en matière de règlement des instruments financiers et sur l'organisation et la conduite des activités des dépositaires centraux des titres (dit règlement « CSDR »), est entré en vigueur en 2014.

Ce règlement a été complété en 2017 d'une série de normes techniques portant par exemple sur les exigences opérationnelles, d'agrément et de surveillance des dépositaires centraux de titres (CSD). Une autre norme technique adoptée en mai 2018, le règlement délégué de la Commission (EU) 2018/1229 sur la discipline en matière de règlement, aurait dû entrer en vigueur vingt-quatre mois après sa publication (25 mai 2018), mais a été reportée une première fois au 1er février 2021 et pourrait désormais être reportée au 1er février 2022 (l'AEMF a publié le 28 août 2020 un rapport sur un nouveau report de la date d'entrée en vigueur du règlement délégué de la Commission (EU) 2018/1299 sur la discipline en matière de règlement au 1er février 2022).

En France, l'AMF et la Banque de France sont les autorités compétentes sous « CSDR » et conduisent conjointement la supervision des CSD établis en France. Les responsabilités de la Banque de France portent principalement sur la finalité des règlements, le règlement en espèces, les liens entre CSD, le risque opérationnel et la politique d'investissement.

La plupart des CSD européens sont aujourd'hui agréés (22 sur 30) et, parmi ceux qui restent, plusieurs démarches sont en cours. Parmi les CSD ayant été agréés, deux CSD sont français : Euroclear France et ID2S.

Après l'agrément, « CSDR » prévoit que les autorités compétentes réexaminent, au moins une fois par an, les dispositifs, stratégies, processus et mécanismes mis en œuvre par les CSD, et évaluent les risques auxquels les CSD sont exposés. Le niveau de détail et la fréquence de cette évaluation sont déterminés par les autorités compétentes en fonction de la taille et de l'importance systémique des CSD, ainsi qu'en fonction de la nature, de l'ampleur, et de la complexité de leurs activités. Les autorités compétentes doivent informer les autorités concernées (en particulier l'Eurosystème) des résultats du réexamen et de l'évaluation.

Depuis 2020, et conformément aux dispositions prévues dans « CSDR », un processus de révision du règlement a été lancé. Les travaux consistent actuellement à identifier les sujets et à définir l'approche générale de cette première révision ; il ne s'agit pas encore de faire une proposition législative d'amendement de « CSDR » (dont le calendrier est à ce jour imprécis).

Le calendrier de la Commission se découpe en deux phases.

- Un premier volet (pour lequel la Commission devrait remettre un rapport le 16 décembre 2020), couvrant des thèmes sélectionnés en priorité car devant être plus simples à traiter : activités transfrontalières et passeports ; règlement internalisé ; exercice de revue régulière (post-agrément) de la conformité et des risques des CSD ; nouvelles technologies, même si une incertitude demeure quant à la capacité à réaliser des amendements sur ce dernier point dès ce premier volet, sachant qu'en parallèle, un certain nombre de travaux sont entrepris par la Commission sur l'innovation. En effet, ce sujet doit être abordé en lien avec les nouveaux projets de règlement de la Commission publiés le 24 septembre 2020, en particulier sur les cryptoactifs (*Markets in Crypto-assets* – MiCA) et celui de « régime pilote » pour permettre des expérimentations avec des dérogations à certaines dispositions du « CSDR » (*cf. encadré 3*).

- Un deuxième volet, qui devrait débuter en 2021, dans lequel la Commission initiera une revue plus exhaustive du « CSDR », en élargissant son spectre au-delà des thèmes identifiés précédemment. La liste des thèmes d'analyse n'est pour le moment pas totalement définie.

1.5 La mise en œuvre de nouveaux principes internationaux dans le domaine de la cyberrésilience

Les cybermenaces constituent plus que jamais un enjeu de résilience de premier plan pour le système financier, et en particulier les infrastructures de marché. Les travaux de renforcement de la cyberrésilience continuent donc de progresser selon deux axes :

- un changement de paradigme lié, d'une part, aux moyens de plus en plus importants dont disposent les organisations malveillantes, d'autre part, à la complexité croissante des systèmes d'information et à l'augmentation du nombre de canaux utilisés pour y accéder. Par conséquent, la sécurisation des systèmes d'information est complexe, dans un contexte d'augmentation du cyberrisque, qui rend nécessaire la capacité à réagir de façon optimale en cas d'incident avéré ;

- la prise en compte de l'interdépendance opérationnelle croissante entre les différents acteurs financiers et du recours à des fournisseurs tiers qui sont, pour certains d'entre eux, devenus critiques à l'égard du secteur financier dans son ensemble et plus particulièrement des infrastructures de marché. Cela se traduit par une prise de conscience que la défaillance du maillon le plus faible peut avoir des impacts sur l'ensemble du secteur financier.

L'objectif est de s'assurer que l'ensemble des acteurs dispose d'un niveau de protection adapté aux menaces, couvrant tous les domaines de la cybersécurité, de l'identification des risques au plan de la reprise d'activité, en passant par la détection des incidents et la réalisation de tests d'intrusions.

L'adaptation des textes internationaux et européens

Au plan international, les pays membres du G7 ont poursuivi les travaux engagés dès 2016 avec la publication en octobre 2018 des éléments fondamentaux pour la gestion du cyberrisque lié aux fournisseurs tiers de services (*fundamental elements for third party cyber risk management in the financial sector*) et les éléments fondamentaux pour la conduite de tests d'intrusion fondés sur les risques (*fundamental elements for threat-led penetration testing*).

- Les éléments fondamentaux pour la gestion du cyberrisque lié aux fournisseurs tiers de services s'adressent à la fois aux entités financières et aux régulateurs du secteur financier. Ils rappellent les éléments clés à prendre en compte lors du choix des fournisseurs, puis dans le cadre du suivi des prestations fournies, en insistant sur l'importance d'intégrer ces fournisseurs dans les dispositifs de réponse aux incidents, de continuité et de reprise d'activité en cas de sinistre majeur. Un accent particulier est également porté sur l'identification des fournisseurs tiers qui, de par la criticité des services fournis et le nombre important d'acteurs auxquels ils fournissent ces services, peuvent présenter un risque systémique pour le secteur financier dans son ensemble.

- Les éléments fondamentaux pour la conduite de tests d'intrusion fondés sur les risques visent à fournir les principes clés à retenir lors de la conduite de ce type de test par les entités financières. Un accent particulier est porté sur la coordination entre les autorités financières des différents pays concernés lors de la conduite de tests internationaux par les entités multinationales.

L'Eurosystème s'est appuyé sur la CPMI-IOSCO *Guidance on cyber resilience for market infrastructures* publiée fin juin 2016 pour mener un travail d'évaluation de la cyberrésilience des infrastructures de marché européennes, en vue de son renforcement.

Les travaux ont consisté à :

- décliner la *Guidance* CPMI-IOSCO précitée pour préciser, dans le cadre d'un document publié au mois de décembre 2018, les attentes des surveillants européens vis-à-vis des systèmes de paiement et des infrastructures de marché en matière de cyberrésilience (*cyber resilience oversight expectations for financial market infrastructures* – CROE) ;

- favoriser le dialogue entre régulateurs et industrie : l'*European Cyber Resilience Board* est un forum stratégique de haut niveau (*strategic high level meeting*) créé en mars 2018 entre régulateurs et industrie au sujet de la cyberrésilience des infrastructures de marché et des fournisseurs de services critiques. Une première réalisation majeure du forum a été le lancement en février 2020 d'une plateforme (*Cyber Information and Intelligence Sharing Initiative* – CIISI-EU) d'échange d'informations cruciales sur l'évolution de la cybermenace, qui vise à protéger le secteur financier européen en renforçant la prévention, la détection et la capacité de réponse aux cyberattaques ;

- créer un cadre harmonisé pour la réalisation de tests d'intrusion de type *red-teaming* [10] : les travaux lancés début 2017 ont permis de publier en mai 2018 le cadre TIBER-EU (*Threat Intelligence-based Ethical Red Teaming*), qui vise à harmoniser les modalités d'exécution des tests de cyberpénétration dans le secteur financier. Ces tests de pénétration jouent un rôle essentiel pour évaluer la capacité de l'entité testée (infrastructure de marché, banque, assurance, prestataire de service critique, etc.) à se protéger, à détecter et à répondre à une cyberattaque avancée. Ce cadre TIBER-EU, destiné à l'usage des autorités autant que des opérateurs et des sociétés spécialisées auxquels elles feront appel, vise notamment à faciliter la conduite de tests internationaux et leur reconnaissance mutuelle par les différentes autorités financières concernées.

Enfin, la Banque de France a participé à la consultation publique conduite par la Commission européenne entre décembre 2019 et mars 2020 sur le thème de la résilience

10 Exercices et simulations où l'équipe adverse (dite *red team*) vient, comme des cyberattaquants, essayer de percer les défenses de l'entité ciblée.

opérationnelle des acteurs du secteur financier face aux cyberattaques. La consultation publique a permis de recueillir le point de vue des parties prenantes sur la nécessité d'apporter des améliorations à l'acquis législatif concernant :

- les exigences en matière de gestion des risques de sécurité notamment liés aux technologies de l'information et de la communication (TIC) ;
- le signalement des incidents ;
- les tests de résilience opérationnelle et informatique ;
- la supervision des fournisseurs de TIC tiers qui offrent leurs services aux établissements financiers.

L'organisation d'un exercice international de simulation de crise

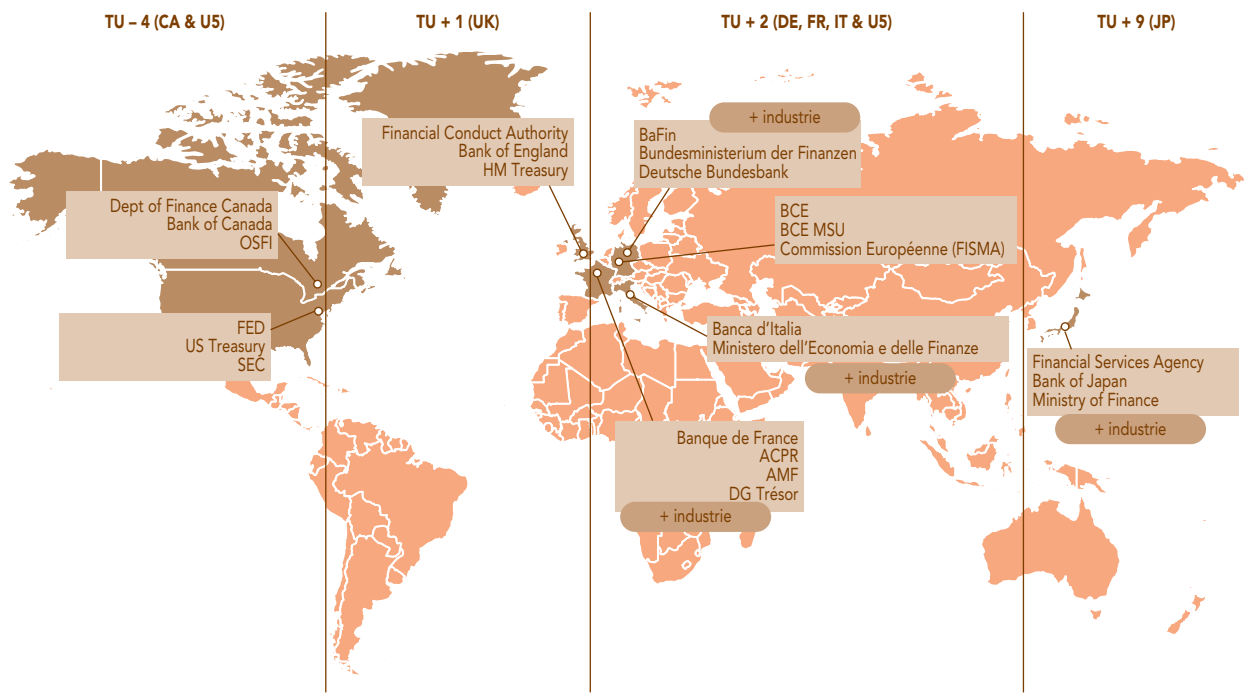
Il est désormais largement reconnu que la très grande interconnexion des différentes places financières au niveau mondial requiert une approche stratégique harmonisée de la cybersécurité de la part des autorités financières. Il apparait notamment, au travers des différents éléments fondamentaux publiés par le G7 [11], que la bonne coordination des actions de réponse et de reprise face à un incident majeur de cybersécurité constitue un des éléments clés de la résilience opérationnelle du secteur financier. Plusieurs juridictions ont déjà mis en œuvre des programmes réguliers d'exercices nationaux, voire régionaux au niveau européen par exemple, mais aucun exercice à très grande échelle n'avait encore été organisé au niveau mondial pour le secteur financier.

C'est la raison pour laquelle les ministres des Finances et les gouverneurs de banques centrales du G7 ont validé en octobre 2017 la proposition de la France, formulée en prévision de la présidence française du G7 en 2019, d'organiser un cyberexercice impliquant les autorités financières – ministères des Finances, banques centrales, autorités bancaires et autorités des marchés – des pays concernés.

L'organisation de l'exercice et le pilotage des travaux préparatoires à l'exercice ont été confiés à la Banque de France.

L'exercice, conduit en temps réel sur une durée de trois jours en juin 2019, a consisté en la simulation d'un cyberincident majeur affectant simultanément plusieurs acteurs du secteur financier. 24 autorités financières du G7 y ont participé, ainsi que des représentants du secteur financier en France, en Allemagne, en Italie et au Japon.

Participants de l'exercice G7 *Cross-Border Coordination Exercise* de juin 2019



Source : Banque de France.

L'exercice a permis, au niveau international, de valider le protocole de communication mis en place entre les autorités financières du G7, notamment dans sa capacité à permettre l'échange des informations les plus pertinentes sur l'incident ainsi que dans sa capacité à faciliter la coordination des actions visant à y répondre et à assurer une reprise coordonnée des services financiers qui soit la plus efficace. En France, il a également permis de valider la résilience du dispositif national de coordination de crise mis en place dans le cadre du groupe de Place Robustesse et d'évaluer l'adéquation des mesures de contingence disponibles.

L'organisation de cet exercice, très complexe par nature et qui constituait une première au niveau mondial, a marqué une grande avancée en matière de coopération internationale. Grâce à son succès, les autorités du G7 sont convenues d'établir un programme d'exercices pour les prochaines années et de publier prochainement des éléments fondamentaux pour la conduite d'exercices de cyberrésilience (*fundamental elements of cyber exercise programs*).

1.6 Les travaux internationaux du CPMI-IOSCO

Ces travaux ont principalement porté sur i) le suivi de la mise en œuvre des PFMI, et ii) l'approfondissement de certaines thématiques couvertes par ces derniers.

Le suivi de la mise en œuvre des PFMI

Ce travail s'appuie sur une approche à trois niveaux.

- Le premier niveau (L1) consiste pour chaque juridiction à autoévaluer l'état d'avancement du processus d'adoption des PFMI en droit local. La grande majorité des juridictions estimant aujourd'hui avoir adopté les PFMI, les travaux se concentrent désormais sur les deux niveaux suivants.

- Le deuxième niveau (L2) consiste à évaluer dans quelle mesure les mesures législatives adoptées dans les différentes juridictions transcrivent complètement les PFMI. Depuis 2017, le groupe de travail du CPMI-IOSCO chargé de suivre la mise en œuvre des PFMI (l'*Implementation Monitoring Standing Group* – IMSG a mené des évaluations de la Suisse, du Canada, des États-Unis (systèmes de paiements et CSD) ; l'évaluation du Brésil, de la Turquie et de l'Union européenne (systèmes de paiements et CSD) sont en cours de finalisation.

- Le troisième niveau (L3) consiste à évaluer la cohérence de la mise en œuvre des PFMI par les infrastructures de marché. Les pratiques des CCP en matière de gestion des risques et plans de rétablissement, ainsi que leur mise en œuvre du « *cover 2* » (dimensionnement des ressources pour faire face au défaut simultané des deux membres les plus importants) ont été évaluées en 2019. L'évaluation des plans de continuité des infrastructures a été menée courant 2019 et 2020, et l'évaluation de leur gestion du cyberrisque a été lancée en 2020.

Si les PFMI se sont bien imposés comme la référence internationale en matière de supervision des infrastructures de marché, en revanche, la robustesse de leur mise en œuvre varie d'une juridiction à l'autre. Les travaux de niveau 2 de l'IMSG, qui se tournent dorénavant vers des juridictions dans lesquelles les marchés financiers sont moins développés et internationalisés, observent des modalités juridiques de « transposition » des PFMI très hétérogènes. Quant aux travaux de niveau 3, ils mettent également en lumière une interprétation parfois divergente de certains termes ou exigences des PFMI ; la production de rapports publics sur chaque thématique étudiée permettra une convergence progressive des interprétations et pratiques par les infrastructures de marché, facteur clé d'une mise en œuvre cohérente des PFMI à travers les différentes juridictions.

L'évolution des standards internationaux

Les travaux menés à cet égard ont notamment porté sur :

- les procédures d'adjudications (ou *auctions*) mises en place par les CCP pour faire face à la défaillance d'un ou de plusieurs de leurs membres. Les analyses menées dans ce cadre ont donné lieu à une publication montrant que, au-delà de la diversité des pratiques, des améliorations pouvaient y être apportées (*cf. encadré 6*) ;

- le cadre de coopération internationale entre autorités. Il s'est notamment agi de faire le point sur les approches actuelles à l'aune des PFMI (et plus précisément les principes fixés dans la « responsabilité E »). Les enseignements tirés de cette analyse ont conduit à publier en décembre 2019 un rapport dressant un état des lieux et rappelant la nécessité pour les surveillants d'infrastructures de marché ayant une activité transfrontalière de pouvoir échanger des informations de manière fluide, en temps normal comme en temps de crise, et ce selon différentes modalités (par exemple grâce à la mise en place de collèges de surveillance) ;

11 Cf. *supra*, 1.5a.

- les modalités d'accès direct aux CCP par les entités non bancaires, comme les assurances et les fonds (accès dit « sponsorisé »), dans le cadre des analyses précédemment menées sur le marché de la compensation pour compte de tiers. Le travail, initié en 2019, devrait aboutir en 2021 sous la forme d'un rapport sur les bénéfices et les risques de ce type de modèle.

2 Le bilan de la surveillance des infrastructures des marchés financiers

La période sous revue a été marquée par la survenance en 2020 de la crise sanitaire liée à la pandémie de la Covid-19, laquelle a rendu nécessaire une adaptation rapide des infrastructures de marché à partir du mois de mars (recours massif au télétravail ; évolution rapide des volumes traités par les infrastructures ; recrudescence des cyberattaques, etc.). Tous ces impacts directs et indirects ont été surveillés de près pour éviter une dégradation de la fourniture de service des infrastructures. Le constat d'ensemble est que les infrastructures, grâce notamment aux cadres de surveillance qui leur sont applicables, ont bien résisté à ces diverses sources de perturbations, et ont continué d'assurer le service des marchés financiers de façon satisfaisante (*cf. encadré 7 « L'impact de la crise liée à la Covid-19 sur l'activité des infrastructures de marché »*).

2.1 LCH SA

LCH SA, la chambre de compensation (CCP) française, propose des services de compensation des instruments financiers et assure la garantie de bonne fin des opérations sur quatre lignes d'activités :

- produits listés au comptant : actions au comptant et obligations convertibles listées sur les marchés Euronext ;
- produits dérivés listés : dérivés actions et dérivés sur matières premières listés sur les marchés Euronext ;
- opérations fermes et pensions sur titres d'État : titres de dette d'États (italien, français, allemand, belge et espagnol). Cette ligne d'activité inclut €GCPlus, le service de compensation de pensions-livrées (*repos*), dont le collatéral est géré de façon tripartite par Euroclear France ;
- *credit default swaps* (CDS) négociés de gré à gré, libellés en euros et en dollars, ayant comme sous-jacents des indices et des entités de référence individuelles [12].

Évolutions récentes et projets de développement

Sur le segment au comptant et dérivés, LCH SA a poursuivi et conforté en 2020 son offre de compensation auprès du marché réglementé Euronext, en accompagnant le développement de l'activité d'Euronext (connexion à la bourse d'Oslo, à la plateforme de marché Optiq, à Euronext Dublin), ou en se connectant à d'autres plateformes de marché comme Turquoise (appartenant au London Stock Exchange Group – LSEG). Pour les dérivés listés, de nouveaux contrats sont aujourd'hui offerts à la compensation : les total return futures sur le CAC 40 depuis octobre 2018, les *market-on-close futures* ou encore les contrats à terme standardisé (ou *futures*) sur indice sur l'immobilier parisien depuis juin 2019.

Les modèles de risque de la CCP ont été adaptés avec l'introduction d'une marge supplémentaire liée au *denetting* de produits réglés et livrés. Le nombre de rachats forcés de titres a été réduit du fait du passage au *trade date netting* (recyclage des instructions en suspens par le CSD Euroclear France, et non plus par la CCP elle-même).

S'agissant de l'activité de compensation sur le segment obligataire (titres de dette publique et *repo*), l'année 2019 a été marquée par la migration de l'offre de compensation en euros depuis LCH Ltd, qui a entraîné une hausse des volumes compensés et des marges collectées. L'offre de services de LCH SA a donc été étendue à de nouvelles dettes en euros. Par ailleurs, les supranationaux disposent désormais d'un modèle d'accès spécifique, dit « *special member* », aux services de LCH SA sur le segment obligataire, utilisé depuis 2020 par la Banque européenne d'investissement.

Concernant l'activité de compensation des *credit default swaps*, la CCP française a poursuivi son développement rapide, et étendu récemment la gamme de produits compensés avec les lancements successifs :

- de CDS sur valeurs financières ou *subordinated financials* (indices et *single names*), en 2018 ;
- de CDS sur *single names* « *senior non-preferred* », constituants des indices iTraxx Europe et iTraxx Senior Financials en 2018 ;
- de *singles names* « *monoline* », qui représentent des *singles names* sur indices que LCH SA peut déjà compenser ;
- des « swaptions » ou options sur indices américains (CDX HY, CDX IG), complémentant ainsi l'offre d'option sur indices européens.

En outre, le segment CDSClear de LCH SA a progressé en matière de parts de marché, puisque la part de LCH SA dans la compensation de ces produits représente désormais en Europe environ 30 % des CDS compensés libellés en euros.

Évaluation

Les autorités nationales compétentes de LCH SA sont la Banque de France, l'ACPR et l'AMF, qui exercent une supervision conjointe en tant qu'autorités compétentes sous le règlement européen EMIR (*cf.* supra, *section 1.1*). LCH SA, qui a par ailleurs le statut d'établissement de crédit, est supervisée à ce titre par l'ACPR ; relevant de la catégorie des « établissements moins importants » (*less significant institutions*, LSI), elle ne fait l'objet que d'une supervision indirecte par la BCE dans le cadre du mécanisme de supervision unique.

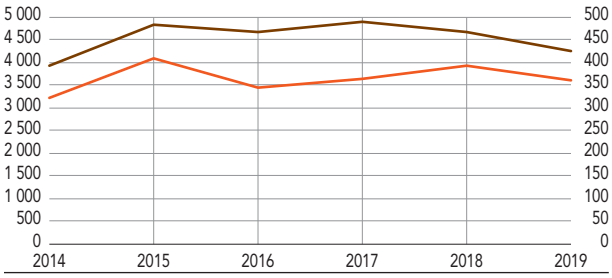
Pour mener à bien leur mission de surveillance, les autorités nationales compétentes réalisent des contrôles sur pièces – par exemple l'étude des projets ou changements proposés par la chambre de compensation –, analysent les informations et données sur l'activité et sur les risques, et organisent des réunions régulières avec les représentants de la chambre de compensation. Des inspections sur place peuvent également être diligentées par l'ACPR.

En vertu de l'article 18 du règlement EMIR, elles doivent par ailleurs associer les autres autorités nationales de l'UE intéressées au bon fonctionnement de l'infrastructure dans le cadre d'un collège de surveillants (« collège EMIR »). Outre les autorités en charge de la surveillance de cette dernière, ces collèges incluent celles qui supervisent les principaux membres compensateurs, les plates-formes de négociation, des contreparties centrales interopérables et des dépositaires centraux de titres, les banques centrales d'émission des principales devises de l'UE traitées, ainsi que l'AEMF, qui ne dispose pas de droit de vote.

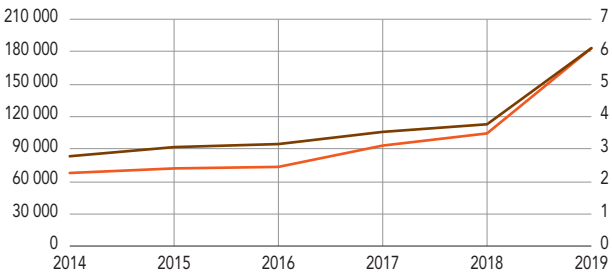
Ce dispositif a pour objectif de permettre à la fois la promotion d'une approche homogène de la mise en œuvre des exigences de l'EMIR au sein de l'UE, une évaluation adéquate des risques de la CCP prenant en compte son profil de risques et les différents segments de marché qu'elle compense, tout en associant les principales autorités concernées des autres pays membres de l'UE. Le collège des autorités est le forum adapté pour échanger des informations sur la chambre de compensation et étudier les changements proposés par cette dernière. Le collège EMIR de LCH SA a été établi en janvier 2014 et comporte 19 autorités (dont l'AEMF), provenant de 9 pays différents

G1 Volumes compensés par LCH SA
(échelle de gauche : notionnel en milliards d'euros ; échelle de droite : nombre de transaction en millions, excepté pour les CDS – graphique d – en unités)

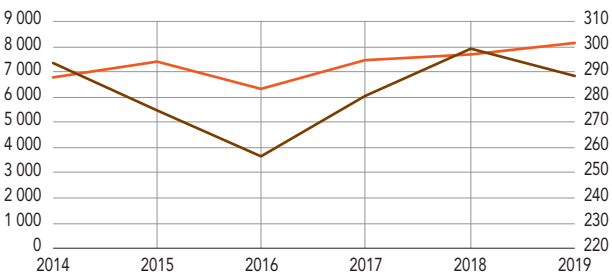
a) *Cash equities*



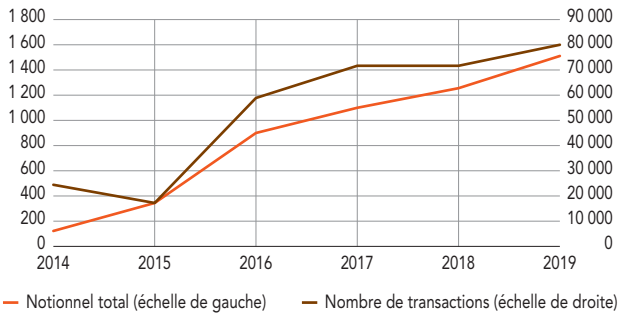
b) *Repo* (*sale and repurchase agreement*, opération de pension)



c) Dérivés listés



d) CDS (*Credit default swaps*)



Source : LCH SA.

12 Les CDS sur indices compensés sont les suivants : iTraxx Europe Main, iTraxx Europe Crossover, iTraxx Europe Senior Financials (et les single names correspondants) ; CDS iTraxx Europe Subordinated Financials ; CDX North America Investment Grade et CDX North America High Yield (et les *single names* correspondants).

de l'UE – la Banque de France en assure la présidence. Les collèges permettent d'échanger avec les autres autorités des informations d'ordre divers, sur le bilan de supervision de l'année écoulée, et de les informer du plan de supervision et des sujets sur lesquels les autorités nationales compétentes ont décidé de mener une analyse approfondie, en plus des projets ou changements qui sont soumis à leur évaluation.

Conformément au règlement EMIR, l'avis du collège, formulé par vote au titre de l'article 19 de l'EMIR, est nécessaire au moment de l'agrément de la CCP, mais aussi dans le cadre des projets d'extension de l'offre de services, d'ouverture de nouvelles lignes d'activités, ou pour les sujets affectant de manière significative le cadre de gestion des risques de la CCP, comme par exemple un changement de modèle de marges. Dans le cadre d'EMIR 2.2, l'AEMF exprimera aussi, notamment, un avis sur les connexions avec une plateforme de négociation, les changements de gouvernance, l'externalisation ou les accords d'interopérabilité.

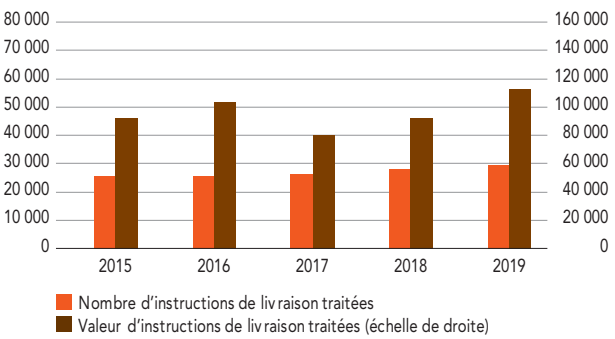
Les autorités françaises organisent une réunion du collège chaque année : trois réunions ont donc été tenues entre 2018 et 2020.

Avec la sortie effective du Royaume-Uni de l'UE au 1er janvier 2021, la Banque d'Angleterre cessera d'être membre de droit du collège EMIR de LCH SA. Étant donné les liens très forts entre la CCP française et la CCP britannique LCH Ltd, il sera nécessaire de continuer d'impliquer les autorités britanniques dans la supervision collégiale de LCH SA. Dans le cadre notamment de la revue des standards de l'AEMF relatifs au fonctionnement des collèges, les autorités françaises étudient actuellement plusieurs options pour faire évoluer l'instance chargée de LCH SA.

2.2 Euroclear France et ESES France

Euroclear France, dépositaire central de titres (CSD), offre les trois « services de base » définis par « CSDR » [13] (voir 1.4), ainsi que plusieurs services dits « accessoires de type non bancaire » [14]. Euroclear France exploite le système de règlement de titres ESES France [15], connecté à T2S depuis septembre 2016. La quasi-totalité des transactions et des opérations sur titres transitent et sont traitées via T2S, auquel Euroclear France externalise le service de règlement de titres et dont il est participant. Les participants à ESES France n'ont de relation contractuelle qu'avec Euroclear France, qu'ils soient techniquement *directly connected parties* ou *indirectly connected parties* en T2S.

G2 Volume et valeur des instructions de règlement-livraison traitées par ESES France
(échelle de gauche : nombre en milliers ; échelle de droite : valeur en milliards d'euros)



Note : ESES, Euroclear Settlement of Euronext-zone Securities.
Source : Banque des règlements internationaux (BRI – BIS Statistics Explorer) – Statistics on payment, clearing and settlement systems in the CPMI countries (Red Book), 2019.

Depuis 2010, Euroclear Nederland et Euroclear Belgium sous-traitent à Euroclear France la gestion opérationnelle de leur activité de règlement-livraison. ESES France traite environ 90 % des valeurs réglées par les trois CSD ESES (Euroclear France, Euroclear Nederland et Euroclear Belgium). D'après les dernières données de l'ECSDA [16], Euroclear France représente 12 % environ des dépôts de titres et 10 % des règlements de titres en Europe. La valeur des 93 000 titres en dépôt en 2019 est de 7 322 milliards d'euros (en hausse de 12 %). La valeur des instructions réglées-livrées en 2019 est de 112 464 milliards d'euros.

Cadre de surveillance

Depuis la mise en œuvre du « CSDR », la Banque de France est non seulement l'autorité de surveillance du système de règlement-livraison ESES France (*Euroclear Settlement of Euronext-zone Securities*), en vertu des pouvoirs qui lui sont donnés par le Code monétaire et financier [17], mais aussi l'autorité nationale compétente pour les dépositaires centraux de titres français. Il s'agit d'une compétence partagée avec l'AMF, qui était déjà l'autorité de supervision d'Euroclear France dans le précédent cadre de surveillance national.

La surveillance conjointe au niveau ESES des systèmes de règlement-livraison (*securities settlement systems*, SSS) et des trois CSD Euroclear France, Euroclear Belgium et Euroclear Nederland, fait l'objet d'un dispositif de coopération entre autorités françaises, belges et néerlandaises. Cette surveillance s'inscrit dans le cadre plus large du protocole d'accord conclu en juillet 2011 entre les autorités du périmètre ESA [18], qui définit les

modalités de coopération et d'échange d'informations entre autorités, en matière de réglementation et de contrôle des opérations de règlement-livraison. La Banque nationale de Belgique a été désignée pour coordonner la coopération. Chacune des autorités nationales compétentes du périmètre ESES conserve toutefois ses prérogatives à l'égard de son CSD national. Ce dispositif de coopération est en cours de révision.

Mise en œuvre du règlement européen « CSDR »

Euroclear France, à l'instar des deux autres CSD ESES, a été agréé au titre du règlement « CSDR » en avril 2019. Son agrément lui a été délivré par l'AMF sur consultation de la Banque de France.

En 2020, conformément aux dispositions de « CSDR », Euroclear France a fait l'objet d'une première procédure annuelle de réexamen et d'évaluation, conduite par les autorités et couvrant la période d'avril 2019 à mars 2020.

ESES France est un système de règlement de titres éligible à l'Eurosystème, et peut donc être utilisé pour les opérations de politique monétaire conduites par la Banque de France.

2.3 ID2S

ID2S est un nouveau dépositaire central de titres français, agréé sous « CSDR » en octobre 2018. Il opère le système de règlement de titres « *Rooster Securities Settlement System* » (RSSS). En août 2020, RSSS est devenu éligible au règlement des opérations de l'Eurosystème, après étude de sa conformité aux critères d'éligibilité.

ID2S intègre la chaîne de blocs dans son système d'information, en lieu et place d'un modèle classique de base de données recensant les informations nécessaires à l'activité de CSD. Il s'agit d'une chaîne de blocs privée lui permettant de valider l'ensemble des transactions.

Le CSD, connecté à T2S depuis fin octobre 2018 (permettant un règlement des transactions en monnaie de banque centrale), offre les trois services de base définis par le « CSDR » : service notarial correspondant à l'émission de titres, service de tenue centralisée de compte titres, et service de règlement de titres pour permettre la circulation des titres.

ID2S ne traite pour l'heure que les titres de créance négociables, plus précisément les NEU CP, titres de maturité courte (un an maximum), pouvant être émis par des entreprises financières ou non financières et par des organismes publics [19] ; à terme, il pourrait étendre son activité à d'autres titres, en particulier les *euro commercial papers* (EuroCP), une autre catégorie de titres de créance négociables émis par les États, des institutions publiques ou des entreprises, essentiellement traités à Londres.

2.4 CORE(FR) et SEPA(EU)

CORE(FR) et SEPA(EU) sont deux systèmes de paiement de détail opérés par STET SA (Systèmes technologiques d'échanges et de traitement).

CORE(FR)

CORE(FR) permet à ses participants, des banques françaises, de présenter leurs opérations de paiement de détail nationales sous la forme de remises groupées pour règlement des soldes nets. Il a été désigné par le Conseil des gouverneurs de la BCE comme un système de paiement d'importance systémique en août 2014, aux côtés des systèmes paneuropéens TARGET2, EURO1 et STEP2-T ; de fait CORE(FR) remplit deux des quatre critères fixés par le règlement UE (n° 795/2014) de la BCE relatif aux exigences de surveillance applicables aux systèmes de paiement d'importance systémique, à savoir la valeur des paiements quotidiennement réglés dans le système (supérieure à 10 milliards d'euros) et la part de marché au regard du volume total des paiements libellés en euros [20]. Ces critères n'ont pas été modifiés par le nouveau règlement (UE) 2017/2094 de la BCE du 3 novembre 2017.

13 « Service notarial » correspondant à l'émission de titres, « service de tenue centralisée de comptes-titres » et « service de règlement » au travers de l'exploitation d'un système de règlement de titres.

14 Gestion des opérations sur titres (versement de coupons et de dividendes…), l'assignation de codes ISIN aux nouveaux titres émis, ou encore la gestion tripartite du collatéral.

15 *Euroclear Settlement of Euronext-zone Securities*

16 *ECSDA - European Central Securities Depositories Association. https://ecsda.eu/*

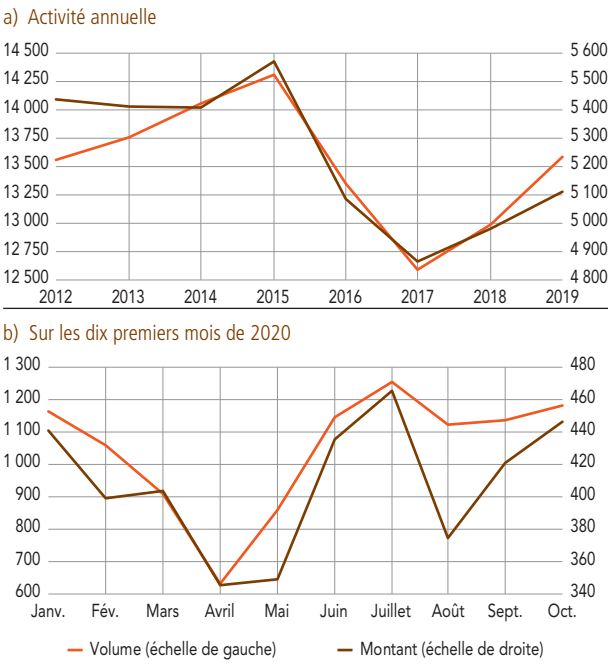
17 Art. L. 141-4. – II : « Dans le cadre des missions du Système européen de banques centrales, […] la Banque de France veille à la sécurité des systèmes de compensation, de règlement et de livraison des instruments financiers. »

18 Pays d'implantation des entités du périmètre Euroclear SA : Belgique, France, Pays-Bas, Royaume Uni / Irlande, Suède, Finlande.

19 Ce marché concerne environ 400 émetteurs et une centaine d'investisseurs institutionnels, pour un encours de 316 milliards d'euros (fin juin 2020). L'activité de négociation est concentrée à 75 % sur le marché primaire, avec une prédominance de négociation de gré à gré intermédiée par des courtiers.

20 Les quatre critères sont : la valeur des paiements quotidiennement réglés, la part de marché, le caractère transfrontalier et la fourniture de services à d'autres infrastructures.

G3 Activité dans CORE (FR)
(échelle de gauche : en millions d'opérations ; échelle de droite : en milliards d'euros)



Source : Banque de France, STET, calculs des auteurs.

Dans le sillage de la décision précitée, la Banque de France a été désignée autorité compétente pour CORE(FR) ; elle est à ce jour la seule banque centrale nationale de l'Eurosystème en charge de la surveillance d'un système de paiement d'importance systémique.

Historiquement, CORE(FR) traitait l'ensemble des moyens de paiement scripturaux, avant la bascule des prélèvements dans le nouveau système SEPA(EU) (*cf.* infra). Aujourd'hui, CORE(FR) continue de traiter la majorité des moyens de paiement qui font l'objet d'une compensation quotidienne permettant de calculer le solde net de chaque participant. Le règlement des positions nettes multilatérales intervient une fois par jour aux environs de 15 h dans TARGET2-Banque de France.

Activité

Sur l'année 2019, environ 13,5 milliards d'opérations ont été compensées dans CORE(FR), représentant en valeur près de 5 112 milliards d'euros, plaçant CORE(FR) au premier rang des systèmes de paiement de détail sur le plan des volumes traités. De 2017 jusqu'à fin 2019, les opérations compensées dans CORE(FR) ont progressé en volume de 7,9 % environ, et en valeur de 5 %, après une baisse de l'activité en 2016 en raison de la bascule des prélèvements sur SEPA(EU). De janvier à octobre 2020, entre 631 et 1251 millions d'opérations ont été réglées mensuellement, représentant des valeurs oscillant entre 345 et 466 milliards d'euros. La grande variabilité des volumes traités en 2020 s'explique par les conséquences du confinement, qui a freiné fortement l'activité des cartes de crédit pendant les mois de mars, d'avril et de mai.

En tant que *Systemically Important Payment System* (SIPS), CORE(FR) s'est doté d'un mécanisme de sécurisation financière au regard du montant important de transactions traitées chaque jour. Cette sécurisation financière se traduit par l'existence d'un fonds de garantie commun (près de 600 millions d'euros depuis le 28 novembre 2019), complété par des appels à garantie individuelle afin de couvrir la position nette débitrice la plus élevée.

Depuis fin février 2013, STET héberge sur la plateforme CORE le Centre d'échange et de compensation (CEC) pour la communauté belge. Il intervient en qualité de prestataire de service critique pour le système géré par le CEC, et surveillé par la Banque nationale de Belgique.

Évaluation

Le rapport d'évaluation de CORE(FR) au regard des exigences du règlement UE n° 795/2014 applicable aux systèmes de paiement d'importance systémique (règlement SPIS) a été finalisé par la Banque de France en 2016. Le système a été jugé globalement conforme et la mise en œuvre du plan d'action a fait l'objet d'un suivi rapproché par la Banque de France et d'un reporting auprès de l'Eurosystème. La clôture du plan d'action a été entérinée par le Conseil des gouverneurs de la BCE en septembre 2019, après la mise en œuvre par STET de toutes les recommandations émises.

Le règlement (UE) 2017/2094 a modifié certains articles du règlement SPIS. Une évaluation d'écart au regard de ces nouvelles dispositions a été menée en 2019. Elle comprenait notamment l'examen des attentes en matière de cybersécurité exposées dans les CROE.

Une évaluation complète a été de nouveau conduite en 2020. Elle intègre les mesures mises en œuvre par l'opérateur, répondant aux recommandations émises dans l'évaluation d'écart de 2019. Ces deux exercices ont conclu à la conformité globale de CORE(FR) au règlement SPIS révisé.

SEPA(EU)

STET a lancé fin 2016 un deuxième système de paiement de détail. Les prélèvements bancaires en format SEPA (appelés *SEPA direct debit* ou SDD) auparavant traités

dans CORE(FR) sont désormais traités et compensés dans SEPA(EU). CORE(FR) et SEPA(EU) sont deux systèmes distincts sur le plan juridique, mais qui présentent néanmoins des caractéristiques communes. SEPA(EU) opère en effet sur la même plateforme technique que CORE(FR) et est régi par une gouvernance identique.

Dans la mesure où SEPA(EU) règle, sur une base annuelle, des volumes de paiement inférieurs à 25 % de la part de marché des paiements domestiques, ce système appartient à la catégorie « autres systèmes de paiements de détail » (*other retail payment systems*, ORPS), d'après la méthodologie de classification élaborée par l'Eurosystème [21]. L'évaluation de cette catégorie est conduite au regard du respect de neuf principes CPMI-IOSCO pour les infrastructures des marchés financiers [22] (PFMI).

Activités dans SEPA(EU)

Sur les dix premiers mois de l'année 2020, environ 2,5 milliards de transactions (prélèvements SDD) ont été réglées dans SEPA(EU), pour un montant de 942 milliards d'euros. Sur l'année 2019, le volume des transactions réglées est resté relativement stable au fil des mois (entre 204 et 249 millions de transactions par mois) et les valeurs mensuelles traitées ont oscillé entre 84 et 122 milliards d'euros environ.

STET a lancé en novembre 2018 une offre de paiements instantanés pour les communautés bancaires française et belge. *CSM Instant Payment* est un service de règlement des virements instantanés répondant au *scheme* développé par l'*European Payment Council*, SCT Inst [23]. Son plafond, initialement fixé à 15 000 euros au niveau interbancaire en France, revu annuellement par l'EPC, a été porté à 100 000 euros en juillet 2020. Au 30 octobre 2020, 18 prestataires de services de paiement en France et en Belgique étaient connectées à IP CSM, couvrant 85 % des comptes de ces deux pays.

Cette offre a été enrichie en février 2020 avec une solution (SWIP *Single Window for Instant Payments*) permettant aux participants de gérer via un accès unique leurs paiements instantanés, y compris lorsqu'ils passent par l'interconnexion proposée par TIPS ou par RT1 (systèmes de paiements instantanés exploités respectivement par l'Eurosystème et par EBA Clearing), permettant ainsi d'atteindre ces deux systèmes paneuropéens.

Évaluation

À la suite de l'évaluation de lancement de SEPA(EU) en juillet 2017, l'opérateur STET a proposé des mesures répondant aux recommandations du surveillant, puis mis en œuvre le plan d'action requis.

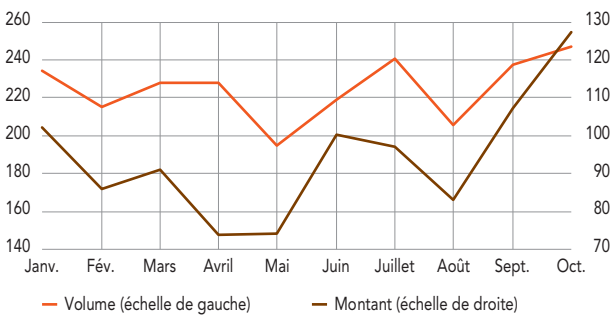
Une mise à jour du rapport d'évaluation de SEPA(EU) au regard des exigences des PFMI applicables aux ORPS a été effectué par la Banque de France en février 2019, dans le cadre du lancement de la fonctionnalité de paiements instantanés. Le système a été jugé conforme aux neuf principes qui lui sont applicables.

Une évaluation de changement mineur a également été conduite en août 2020, à la suite du lancement de la fonctionnalité SWIP. Ce changement n'a pas impacté la conformité du système.

2.5 La surveillance coopérative

La Banque de France participe également à la surveillance coopérative de plusieurs infrastructures de marché et fournisseurs de services critiques établis dans d'autres pays, ou de dimension paneuropéenne voire internationale.

G4 Activité dans SEPA(EU) en 2020
(échelle de gauche : volume en millions ; échelle de droite : montant en milliards d'euros)



Source : «Banque de France, STET, calculs des auteurs.

21 *https://www.ecb.europa.eu/pub/pdf/other/Revised_oversight_framework_for_retail_payment_systems.pdf*

22 Les neuf principes considérés sont la base juridique (principe 1), la gouvernance (principe 2), le cadre de gestion intégrée des risques (principe 3), le caractère définitif du règlement (principe 8), les règles et procédures applicables en cas de défaut d'un participant (principe 13), le risque opérationnel (principe 17), les conditions d'accès et de participation (principe 18), l'efficience et l'efficacité (principe 21) ainsi que la communication des règles, procédures clés et données de marché (principe 23).

23 L'EPC SCT Inst est un *scheme* paneuropéen fondé sur le virement SEPA. Cet ensemble de règles et procédures vise à lutter contre le morcellement du marché européen du paiement de détail. Le *scheme* SCT Inst impose le traitement d'une transaction en moins de 10 secondes, 365 jours par an, 7 jours sur 7 et 24 heures sur 24.

TARGET2

TARGET2 est, depuis 2008, le système RTGS (système à règlement brut en temps réel) de la zone euro. Le système a été développé par trois banques centrales : la Banque de France, la Deutsche Bundesbank et la Banca d'Italia. En 2020, le système relie 24 banques centrales nationales (ainsi que la BCE) et leurs communautés nationales d'utilisateurs. Les banques centrales participantes regroupent les 19 banques centrales de la zone euro et 5 autres banques centrales de pays de l'UE n'appartenant pas à la zone euro, à savoir la Bulgarie, la Croatie, le Danemark, la Pologne et la Roumanie.

À l'instar du système français CORE(FR), TARGET2 a été identifié comme un système de paiement d'importance systémique par une décision du Conseil des gouverneurs d'août 2014. Il est donc soumis aux exigences du règlement SPIS révisé BCE n° 2017/2094 du 3 novembre 2017. La BCE assure la coordination de la surveillance de TARGET2 avec la coopération des banques centrales nationales participantes au système.

Une évaluation d'écart au règlement SPIS révisé a été menée en 2020, sous l'égide de la BCE et de façon conjointe les banques centrales de la zone euro volontaires pour mener l'exercice d'évaluation. Plusieurs actions doivent être entreprises par l'opérateur pour assurer la pleine conformité du système à toutes les dispositions du règlement révisé. L'opérateur de TARGET2 s'est engagé à mettre en œuvre les mesures demandées, qui feront l'objet d'un suivi et d'une communication rapprochés par la BCE. Certaines de ces actions pourraient toutefois n'être achevées que lors de l'implémentation de la future plateforme technique consolidée (*cf.* infra).

La cyberrésilience du système TARGET2 (article 15.4 a du règlement SPIS) fait l'objet d'un traitement particulier. L'évaluation en cours sera finalisée début 2021. La conformité est jugée selon la méthodologie CROE.

Afin de favoriser le développement des paiements instantanés en Europe, l'Eurosystème a lancé en novembre 2018 une solution de règlement des paiements instantanés avec la création de TIPS (*TARGET Instant Payment Settlement*), en tant que nouveau service au sein de TARGET2. TIPS traite directement les paiements instantanés intervenant entre deux de ses participants, en s'appuyant sur une procédure de paiement en temps réel.

En tant que service de TARGET2, TIPS est soumis à une surveillance continue de l'Eurosystème. L'inclusion prochaine de nouvelles devises autre que l'euro dans TIPS a incité à élargir les modalités de sa surveillance en créant le *TIPS Currencies Oversight Group*. Ce groupe inclura en plus de l'Eurosystème les banques centrales émettrices des devises traitées dans TIPS, en premier lieu la couronne suédoise.

T2S

Si T2S ne correspond pas à la définition de « système » de règlement de titres au sens de la directive finalité des règlements, et n'est donc pas surveillé à ce titre, son caractère systémique en tant que plateforme paneuropéenne de règlement de titres a conduit l'Eurosystème à appliquer un dispositif de surveillance analogue à celui des systèmes de règlement de titres. La BCE est le surveillant principal de T2S, avec la participation active et la validation de l'approche et des conclusions par l'ensemble des banques centrales nationales. En 2019, T2S avait réglé 154 769 117 transactions (pour une valeur totale de 282,06 trillions d'euros).

La surveillance de T2S est par ailleurs opérée de façon conjointe par les banques centrales et les autorités des marchés financiers des différentes juridictions dans lesquelles un CSD au moins s'est engagé contractuellement à externaliser son service de règlement-livraison à T2S, avec une coprésidence de cette instance coopérative du groupe de surveillance par la BCE et par l'AEMF. Aux 24 CSD ayant migré lors des cinq vagues initiales de migration à T2S, se sont ajoutés ID2S (CSD français) et VP Securities (CSD danois) le 29 octobre 2018. Le T2S *Cooperative arrangement* réunit donc désormais, en plus de l'AEMF et de la BCE, 22 banques centrales et 22 autorités nationales de marché relevant de l'UE et de l'Espace économique européen.

Évaluation de T2S au regard des PFMI

Une évaluation de surveillance exhaustive de T2S au regard des PFMI, engagée en 2018, s'est achevée début 2020. Les quelques recommandations et observations issues de cette évaluation ont donné lieu à un plan d'action dont la mise en œuvre est assurée par l'opérateur T2S.

SWIFT

SWIFT (*Society for Worldwide Interbank Financial Telecommunication*) est le principal fournisseur mondial de services de messagerie standardisée de transfert interbancaire, notamment dans les domaines des paiements et des titres. Au regard de sa dimension internationale et son rôle clé dans les échanges financiers impliquant la quasi-totalité des acteurs du secteur financier mondial, SWIFT fait l'objet d'une surveillance coopérative régie par un accord entre les banques centrales du groupe des

dix (G10). La Banque nationale de Belgique, en tant que surveillant principal ou *lead overseer*, assure la coordination de cette surveillance à laquelle la Banque de France participe activement.

SWIFT a lancé en 2016 le *Customer Security Programme* (SWIFT CSP) à destination de tous ses clients. Il vise à améliorer la cyberrésilience des infrastructures connectées à SWIFT et des entités financières utilisatrices, au travers d'exigences concernant principalement la gouvernance de la cybersécurité, la prévention, la détection et la réponse aux incidents.

Les travaux de surveillance de la période sous revue ont notamment porté sur le renforcement progressif des exigences sécuritaire du *Customer Security Programme*, les mesures mises en œuvre par SWIFT pour s'assurer de la conformité de ses clients vis-à-vis des exigences du CSP, le programme d'adoption du standard ISO 20022 [24] et les mesures prises pour assurer la continuité et la sécurité opérationnelle des opérations lors de la crise Covid-19.

CLS

Le système CLS permet le règlement en mode PVP (paiement contre paiement) des instructions de paiement sur des transactions du marché des changes au comptant (« *spot* »), sur certains dérivés listés et sur des *swaps* de devises. Chaque participant au système possède un compte multidevises ouvert dans les livres de CLS Bank International, avec les positions par devise traitée dans le système. CLS Bank International détient pour sa part des comptes sur les livres des différentes banques centrales émettrices des devises concernées. Le système CLS a commencé son activité de règlement en septembre 2002. Fin 2020, il compte 18 devises éligibles.

Au regard de sa dimension internationale impliquant de nombreuses devises, le système CLS fait l'objet d'une surveillance coopérative régie par un accord (« *the Protocol* ») entre les banques centrales, celles du G10, et les banques centrales dont la devise est traitée par CLS. La Réserve fédérale assure la coordination de cette surveillance en tant que surveillant principal (*lead overseer*). Le dispositif de coopération a pour objectif de permettre aux banques centrales concernées de participer à la surveillance du système, afin de s'assurer de sa sécurité et de son efficacité. C'est dans ce cadre que les banques centrales vérifient la conformité de CLS aux normes applicables aux systèmes de paiement et aux infrastructures de marché, et examinent les changements proposés par l'opérateur afin d'évaluer les éventuels impacts sur les règles et les conditions du fonctionnement du système, notamment sur son profil de risques. Le comité de surveillance (*oversight committee*), placé sous l'égide de la Banque fédérale de Réserve de New-York (FRBNY), et auquel participent les banques centrales signataires, dont la Banque de France, permet d'assurer cette coopération.

EURO1 et STEP2-T

Sous l'égide de la BCE, qui assume le rôle d'autorité compétente, la Banque de France participe à la surveillance coopérative des systèmes de paiement paneuropéens exploités par la société EBA Clearing : EURO1 (système de paiement de montant élevé), STEP2-T (système de paiement de détail pour le traitement des virements SCT et des prélèvements SDD) et RT1 (système de paiement de détail pour le traitement des virements instantanés SCT Inst).

La Banque de France a contribué à différents travaux d'évaluation conduits par la BCE, concernant notamment la conformité de EURO1 et STEP2-T à la réglementation sur les systèmes de paiement d'importance systémique qui a été révisée en 2017 (*cf.* supra*, section 1.3*) et aux attentes en matière de cyberrésilience (*cf.* supra*, section 1.5*), ainsi que le suivi des plans d'action, dont celui émis dans le cadre de l'évaluation de RT1, le système paneuropéen de paiement instantané d'EBA Clearing.

Les CCP établies dans d'autres pays de l'Union européenne

La Banque de France est membre des collèges EMIR de plusieurs CCP européennes, au titre de l'article 18 du règlement EMIR. Pour la période sous revue, elle a ainsi participé aux collèges de la CCP italienne CC&G (Cassa di Compensazione e Garanzia), avec qui la CCP française a un lien d'interopérabilité, de la CCP allemande Eurex Clearing AG, de la CCP néerlandaise EuroCCP et de la CCP britannique LCH Ltd en tant que surveillant du dépositaire central de titres (Euroclear France), auquel ces CCP sont liées. Au-delà des frontières européennes, la Banque de France a également participé, avec l'ACPR et l'AMF, au *Crisis Management Group* de la CCP américaine CME.

24 ISO 20022 est une norme ISO régissant l'échange de données informatisé entre les institutions financières, principalement utilisée dans les domaines des paiements et des titres

ENCADRÉS

❶ L'impact du Brexit sur les chambres de compensation

La décision du Royaume-Uni de sortir de l'Union européenne (UE) et de l'Espace économique européen (EEE), entrée en vigueur le 1er février 2020, a des implications importantes pour la réglementation et la supervision des infrastructures de marché qui y sont établies. En particulier, certaines contreparties centrales (CCP) britanniques sont d'une importance systémique très significative pour l'UE à 27, notamment LCH Ltd (qui compense 80 % du marché mondial des swaps de taux en euros) et ICE Clear Europe Ltd (qui compense 99 % des dérivés listés de taux courts en euro, et 70 % des *credit default swaps* – CDS – européens).

Le premier point d'attention dans la période de négociation de 2017 à 2020 a consisté à éviter tout « effet falaise » en matière de compensation centrale. Dans cette perspective, des mesures de reconnaissance temporaire en cas de Brexit dur ont été prises par les autorités européennes et françaises en 2019. Si l'obtention d'un accord de transition fin 2019 a permis de sortir de cette hypothèse et d'éviter l'effet falaise en février 2020, l'état des négociations a rendu nécessaire le renouvellement de certaines mesures à partir de septembre 2020.

Un deuxième enjeu est celui de la supervision des CCP britanniques post Brexit. En effet, ces CCP sont aujourd'hui soumises au règlement EMIR (*European Market Infrastructures Regulation*), qui comporte des exigences prudentielles supérieures aux standards internationaux, et sont supervisées par la Banque d'Angleterre. Celle-ci anime les collèges de supervision prévus par l'EMIR, qui rassemblent les autorités européennes principalement intéressées, dont la Banque, l'Autorité de contrôle prudentiel et de résolution (ACPR) et l'Autorité des marchés financiers (AMF), notamment au titre de la supervision des adhérents compensateurs français, et la Banque centrale européenne (BCE) en tant que banque centrale d'émission de l'euro.

Après la sortie du Royaume-Uni de l'UE et de l'EEE, on ne peut exclure, à terme, d'éventuelles divergences réglementaires entre le régime britannique encadrant les CCP et le droit communautaire. De plus, les textes précisant l'EMIR (règlements techniques, etc.) pourraient ne plus être appliqués au Royaume-Uni dans leur intégralité. Consciente de ces risques, la Commission européenne a accordé une reconnaissance temporaire (jusqu'à fin juin 2022) du cadre réglementaire du Royaume-Uni. Si cette reconnaissance devait ne pas être renouvelée, les CCP britanniques ne seraient plus autorisées à servir des participants européens, sauf à relocaliser au moins partiellement leur activité (en particulier leurs activités en euros) dans l'UE.

Sur le fondement de cette déclaration d'équivalence, LME Clear a été classé en Tier 1 et LCH Ltd et ICE Clear Europe Ltd en Tier 2, à l'issue du processus de catégorisation des CCP britanniques conduit par l'Autorité européenne des marchés financiers (AEMF) en septembre 2020.

À moyen terme, la relocalisation des segments les plus systémiques est également souhaitable dans l'optique de protéger la stabilité financière européenne. En effet, une CCP qui effectue des opérations libellées en euros, ou dans une autre devise de l'UE, mais qui n'est pas principalement contrôlée par une autorité européenne, est susceptible de prendre ou de se voir imposer par son autorité de contrôle nationale des mesures qui ne sont pas dans l'intérêt de la stabilité financière de l'UE. C'est une leçon tirée de l'expérience passée, notamment dans le cadre de la crise des dettes souveraines de la zone euro. Au total, la perspective du Brexit et le risque de divergence avec le cadre réglementaire européen renforcent la nécessité de relocaliser dans l'UE la compensation des instruments libellés en devises de l'UE qui revêtent une importance stratégique, à la fois pour la mise en œuvre de la politique monétaire, le financement de l'économie et la stabilité financière dans la zone.

Dans cette perspective, LCH Ltd et ICE Clear Europe Ltd feront l'objet d'une nouvelle évaluation par l'AEMF courant 2021, afin de déterminer si elles sont d'une importance systémique substantielle pour l'UE. Cette évaluation pourra déboucher sur une non-reconnaissance au titre de l'art. 25 (2c) de l'EMIR, pouvant entraîner (tout comme le non-renouvellement de l'équivalence) une relocalisation sur le continent européen de leurs activités désignées comme systémiques.

❷ Le règlement européen sur le rétablissement et la résolution des CCP (CCPRR)

D'après ce nouveau règlement, chaque CCP devra désormais disposer d'un plan de rétablissement et d'un plan de résolution, qui devront permettre, en cas de défaillance, de maintenir les fonctions critiques de l'infrastructure pour la stabilité financière, en évitant le recours aux fonds publics.

a) Le renforcement du capital des CCP en continuité d'exploitation

Le texte introduit un « *second skin in the game* » (SIG), qui constitue une part des ressources propres de la CCP, qui aura vocation à être utilisé juste avant les outils de rétablissement, après épuisement de la cascade de défaut, pour faire peser une partie des pertes sur les actionnaires en rétablissement. Pour satisfaire les plus petites CCP, qui pourraient avoir des difficultés à lever le capital supplémentaire, et pour éviter les inégalités de concurrence au niveau international, le montant de ce second SIG n'est pas fixé, mais devra être compris entre 10 et 25 % des exigences de capital. Il revient à l'Autorité européenne des marchés financiers (AEMF) et à la Commission européenne de préciser, par des normes techniques de réglementation, les règles gouvernant la méthodologie de calcul de ce second SIG, en prenant en compte une série d'éléments listés dans le règlement (par exemple les activités de la CCP, la politique de réinvestissement du collatéral, ou la structure des incitations dans l'écosystème de la CCP).

b) Les outils de rétablissement

Les plans de rétablissement des CCP européennes devront inclure des outils d'allocation des pertes aux membres, comme les décotes sur marges de variation dues par la CCP (*variation margin gain haircutting* – VMGH) ou la résiliation partielle ou totale des contrats (*tear-up*). En cas de rétablissement, la CCP sera tenue de suspendre les dividendes, rachats d'action et le superviseur pourra également suspendre les rémunérations variables.

c) Les outils de résolution

Le texte prévoit six outils. Trois sont communs avec le régime bancaire : ce sont la dépréciation ou la conversion des instruments de fonds propres et des titres de dette, la cession d'activité et la CCP-relais. Les trois autres sont les appels de liquidité (cash calls) ainsi que les VMGH et tear-up déjà cités.

Le texte ne contient pas, notamment, deux outils controversés : i) la décote sur les marges initiales (*initial margin haircutting* – IMH), qui aurait pu créer une exposition importante des participants et une incitation à sortir de la CCP dès qu'un participant fait défaut ; et ii) l'allocation forcée des positions, qui aurait pu conduire à imposer à certains acteurs de prendre des positions qu'ils ne sont pas capables de gérer (cet outil n'est mentionné que dans un considérant).

d) La flexibilité dans l'utilisation des pouvoirs de résolution

Le texte prévoit la flexibilité dans la mise en œuvre des outils de résolution par l'autorité, afin de pouvoir répondre à des situations par définition difficiles à anticiper, mais dans lesquelles les enjeux de stabilité financière seront élevés.

e) Le principe du *no creditor worse off* (NCWO)

Le principe du NCWO prévoit qu'un créancier ne puisse être traité moins favorablement en cas de résolution qu'il ne l'aurait été en cas de liquidation ou d'application stricte des règles de la CCP (le « contrefactuel »). Ceci correspond, pour les CCP, à l'échec du plan de rétablissement, qui aboutit, i) dans un scénario de défaut d'un ou de plusieurs membres compensateurs, à la résiliation de l'ensemble des contrats ou « *full tear-up* » des contrats du service de compensation dont le processus de gestion du défaut a échoué, et ii) dans un scénario où les pertes ne sont pas dues à un défaut de membre compensateur, à la liquidation de la CCP. Les « coûts de remplacement » des contrats en cas de « *full tear-up* » devront être pris en compte pour refléter la valeur que préserve l'autorité de résolution en maintenant la continuité de ces contrats. Ils seront définis par une norme technique de réglementation proposée par l'AEMF et adoptée par la Commission européenne, sur la base de critères les plus objectifs possibles.

f) L'indemnisation des participants qui subissent des pertes en résolution

La capacité de l'autorité de résolution à obliger la CCP à indemniser les membres qui ont dû contribuer en résolution au-delà de leurs engagements contractuels, dans les limites permises par l'application du NCWO, a été adoptée dans le règlement final.

g) Gouvernance du rétablissement et de la résolution dans l'Union européenne

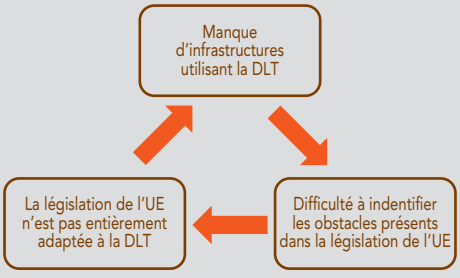
Le texte prévoit que les collèges EMIR mis en place pour l'agrément des CCP valident le plan de rétablissement des CCP, et que les collèges de résolution des CCP approuvent le plan de résolution. En cas de désaccord au sein des collèges, l'autorité compétente ou l'autorité de résolution, respectivement, prendrait la décision définitive. Une majorité simple peut saisir l'AEMF. L'ensemble des pouvoirs de l'AEMF seront exercés, en son sein, par le « *Resolution Committee* » (comité de résolution), créé par le texte.

❸ Le projet de régime pilote (*pilot regime regulation* – PRR) pour les infrastructures de marché

L'adaptation de la réglementation aux nouveaux enjeux de l'innovation (notamment la place des fintechs) semble incontournable pour positionner l'Europe du futur, servir l'économie, les citoyens et les entreprises.

Le 24 septembre 2020, dans le cadre de son paquet sur la finance digitale, la Commission européenne a proposé, en complément de dispositions spécifiques sur les cryptoactifs (*Markets in Crypto-assets* – MiCA) et sur la résilience opérationnelle digitale du secteur financier (*Digital Operational Resilience Act* – DORA), la mise en place d'un régime pilote pour les infrastructures de marché recourant aux technologies de registres distribués ou chaînes de blocs.

Le projet de PRR (*pilot regime regulation*) participe de l'ambition de la Commission, tout en assurant la stabilité financière, la protection des investisseurs et l'intégrité des marchés, de rompre un cycle dans lequel l'adaptation du cadre législatif pour permettre l'usage de technologies innovantes peinait à être menée, car le développement de ces technologies était entravé par des obstacles législatifs :



Source : Commission européenne.

L'objectif du régime pilote est ainsi de permettre le développement d'un marché secondaire pour les cryptoactifs et l'émergence de cas d'usage de technologie innovante (i.e. *blockchain* et plus largement technologie de registres distribués autrement appelée « *distributed ledger technology* » ou DLT) dans le règlement livraison.

Le texte, actuellement en cours de discussion, propose un régime temporaire dérogatoire à certaines des obligations normalement applicables à deux types d'acteurs : les plateformes de négociation (MTF) et les systèmes de règlement livraison (SSS) – généralement exploités par les CSD. Il est entendu que les exemptions ne seraient applicables qu'à des MTF et SSS fondés sur des technologies innovantes et faisant la démonstration d'un besoin réel, sur autorisation de leur autorité compétente et avis de l'AEMF.

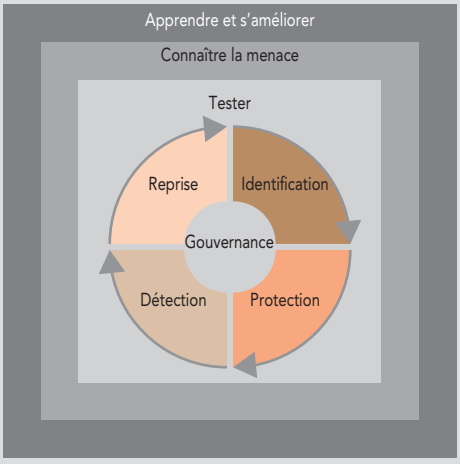
Le régime pilote couvre par ailleurs un large périmètre d'instruments financiers, à l'exception de la dette souveraine. Plus précisément, il vise des titres peu liquides avec deux conditions : que la capitalisation de

l'émetteur soit inférieure à 200 millions d'euros, et que des obligations ne soient admises que si le montant de l'émission est inférieur à 500 millions d'euros. En outre, le PRR fixe des plafonds globaux à chaque expérimentation (la valeur totale des valeurs mobilières devra rester inférieur à 2,5 milliards d'euros), au-delà desquels devraient être déclenchés des plans de transition pour revenir au cadre classique.

À ce stade, le point d'attention majeur concerne la place que le projet réservera au principe du recours en priorité au règlement en monnaie de banque centrale (comme préconisé par les PFMI), notamment pour que les expérimentations se fassent préférentiellement en monnaie numérique de banque centrale et, seulement si celle-ci n'est pas disponible en pratique, en monnaie numérique de banque commerciale. Cela est également nécessaire pour assurer une bonne articulation du PRR avec les expérimentations actuellement conduites par les banques centrales, dont la Banque de France sur une monnaie numérique de banque centrale pour les règlements interbancaires de gros montants.

❹ Les exigences de surveillance en matière de cyberrésilience des infrastructures de marché financiers (CROE)

Afin de permettre une évaluation de la maturité des infrastructures de marché européennes en matière de cyberrésilience dans un cadre commun européen, et d'en suivre l'évolution dans le temps, l'Eurosystème s'est appuyé sur la *Guidance* CPMI-IOSCO publiée en 2016 pour établir un référentiel d'exigences. Établi à partir des huit composantes de la cyberrésilience [1] et sur la base des bonnes pratiques de chaque domaine, ce référentiel de près de 300 critères détaille les attentes des surveillants, de manière plus détaillée et concrète, et indique les voies de progrès à plus long terme pour les infrastructures de marché. S'inscrivant dans la logique et dans le périmètre de la *Guidance* CPMI-IOSCO, l'appréciation du niveau de maturité devient plus transparente, le dialogue entre assujettis et surveillants devient plus concret, et les exigences minimales peuvent être plus facilement adaptées aux différents profils (SPIS, etc.).



Source : BCE - Cyber Resilience Oversight Expectation, page 7 https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf.

Comme dans la *Guidance* CPMI, trois niveaux de maturité sont définis de manière incrémentale, c'est-à-dire que l'atteinte d'un niveau supérieur implique de satisfaire l'ensemble des critères des niveaux inférieurs. La cybermenace étant en constante évolution, les exigences sont fondées sur l'application du principe de l'amélioration continue : pour le niveau *Evolving*, les institutions doivent démontrer l'adaptation de leurs outils et de leur organisation à la gestion du risque cybersécurité, dans le cadre fixé par le conseil d'administration ; pour le niveau *Advancing*, il est demandé que la gestion du risque soit outillée et intégrée aux lignes métier, de manière à obtenir une proactivité vis-à-vis de la menace ; enfin, au niveau *Innovating*, l'infrastructure est reconnue pour sa capacité à insuffler et à partager les meilleures pratiques vers les différentes parties prenantes, au bénéfice de l'ensemble de l'écosystème du secteur financier.

1 Gouvernance, identification, protection, détection, réponse et reprise, test, connaissance de la situation, apprentissage et amélioration continue.

Structurées sur les mêmes catégories de gestion du risque que le référentiel NIST [2] et la *Guidance* CPMI, les exigences sont regroupées par chapitre selon une logique symbolisée par le schéma ci-dessus.

Chaque chapitre commence par une introduction de haut niveau s'inspirant directement des CPMI et permet de comprendre la portée et les intentions des exigences. Cette segmentation en huit chapitres met clairement en relief les forces et les axes d'amélioration de l'infrastructure évaluée, permettant un dialogue plus direct avec le surveillant. Il convient néanmoins d'adopter une approche globale pour atteindre le niveau requis, chaque domaine interagissant avec les autres.

Cette version initiale du référentiel a été appliquée en 2020 sur plusieurs systèmes de paiement d'importance systémique. Le premier retour d'expérience sur les quatre systèmes de paiement européens d'importance systémique (évaluations conduites courant 2020) est favorable, notamment parce qu'il s'inscrit dans une démarche d'amélioration à court, moyen et long terme. L'évaluation des autres infrastructures se fera progressivement, dans l'esprit qui a guidé la création de ce référentiel : la transparence et la clarté des attentes des superviseurs, ainsi que l'amélioration de la résilience de l'ensemble du secteur financier européen.

2 National Institute of Standards and Technology. Cf. NIST, *Framework for Improving Critical Infrastructure Cybersecurity*.

❺ La proposition législative de la commission sur la résilience digitale (*Digital Operational Resilience Act* – DORA)

Après une phase de consultation publique début 2020, la Commission européenne a publié le 24 septembre 2020 un ensemble de projets de textes législatifs visant à promouvoir la transformation numérique de la finance, dont le projet de règlement européen DORA. Ce règlement constitue le versant « sécuritaire » de cette initiative, actant que le cyberrisque est devenu systémique pour le secteur financier.

DORA vise à définir un socle législatif commun s'appliquant à la quasi-totalité du secteur financier, entendu au sens large. Cela recouvre donc des entités très diverses, aussi bien en termes d'activité que de taille : établissements de crédit, établissements de paiement, établissements de monnaie électronique, entreprises d'investissement, prestataires de services sur actifs numériques, CCP, CSD, plateformes de négociation et marchés réglementés, *trade repositories*, compagnies d'assurance et de réassurance (et intermédiaires), fonds de pension, agences de notation, commissaires aux comptes, administrateurs de taux de référence et financement participatif (*crowdfunding*).

Concrètement, DORA vise à harmoniser « par le haut » toutes les dispositions existantes qui figurent actuellement dans un grand nombre de textes sectoriels (directives, règlements), généralement organisés en silos propres à chaque catégorie d'acteurs. D'application directe, le texte s'articule autour de quatre axes : i) les exigences liées à la gouvernance et la gestion du risque informatique ; ii) la notification des incidents de sécurité ; iii) les tests de sécurité ; et iv) la gestion du risque informatique de tiers. Viennent également s'ajouter des considérations sur l'échange d'informations et la coopération entre autorités. Cette harmonisation permettra de mettre fin aux écarts et redondances entre réglementations sectorielles, sources de distorsions de concurrence et d'arbitrages réglementaires.

DORA s'appuie sur un principe de proportionnalité. D'une part, il existera des exemptions en matière de gestion du risque informatique pour les microentreprises et, d'autre part, des obligations comme la conduite des tests avancés ne concerneront que certaines entités jugées systémiques.

Enfin, la gestion des risques liés aux prestataires informatiques (ou « risque informatique de tiers ») constitue la véritable innovation institutionnelle de ce règlement et, en particulier, la mise en place d'une surveillance directe par les autorités d'une sélection de prestataires identifiés comme particulièrement importants pour le secteur financier. Néanmoins, chaque institution financière sera pleinement responsable de sa conformité à DORA, même si elle sous-traite certains services à des prestataires informatiques.

❻
Les bonnes pratiques en matière de vente aux enchères des CCP

La maîtrise du risque de contrepartie étant fondamentale pour les CCP, gérer l'éventuel défaut d'un membre compensateur fait partie de leur cœur de métier. Lorsqu'un défaut survient, la CCP doit réallouer les portefeuilles du membre défaillant dans un temps très court (quelques heures ou jours). Pour ce faire, elle peut soit liquider directement ces positions sur le marché, soit les vendre aux enchères à d'autres membres (*default management auction*). C'est à la fin de ce processus que la CCP détermine les pertes définitives liées au défaut du membre, qu'elle fera absorber par la cascade de défaut (marges du membre défaillant, puis une part de capital de la CCP – *skin in the game* –, puis le fonds de défaut mutualisé). Des offres raisonnables (*i.e.* suffisamment élevées) des participants pour le portefeuille défaillant permettent donc *in fine* de limiter les pertes absorbées par la communauté des membres.

En septembre 2018, la gestion par la CCP suédoise Nasdaq Clearing du défaut d'un trader individuel a conduit à l'absorption par le fonds de défaut d'un montant important de pertes (plus de 100 millions d'euros). La vente aux enchères des positions du membre par la CCP a notamment été critiquée, ce qui a réaffirmé le fort intérêt des travaux du CPMI-IOSCO sur le sujet, lancés au début de l'année 2018.

Cela a conduit à initier un travail d'identification des pratiques des CCP en matière d'enchères, notamment leurs enjeux opérationnels, de dégager des définitions communes et de décrire les points de vigilance attendus. Ce travail a été mené en étroite relation avec l'industrie dans le cadre notamment de *workshops* et de questionnaires, avant d'aboutir à la publication en juin 2019 d'un document consultatif [1] puis, dans le sillage des réactions que celui-ci a suscitées, d'un rapport définitif public en juin 2020 [2].

Le rapport présente d'abord les attentes en matière de gouvernance, avec le besoin de délégations claires du conseil d'administration et l'utilité des groupes de gestion du défaut (DMG) comprenant des participants externes. Pour maximiser les chances de succès d'une vente aux enchères, la CCP doit définir à l'avance sa stratégie de couverture (*hedging*) du portefeuille, afin d'en réduire son risque et le rendre donc plus attractif pour les acheteurs. Elle peut également diviser le portefeuille en plusieurs lots pour en faciliter l'absorption. Les différentes formes d'enchères sont précisées (hollandaises, américaines, à double prix à l'achat et à la vente, etc.) avec leurs avantages respectifs en matière de confidentialité ou de qualité potentielle des offres reçues. L'importance d'une large base de participants aux enchères est soulignée ; des outils incitatifs peuvent être employés à cette fin (par exemple la participation obligatoire, ou la « juniorisation » des contributions au fonds de défaut des membres les moins coopératifs). La CCP doit conduire des exercices (*firedrills*) fréquents pour tester l'ensemble du processus opérationnel ; à partir de la crise de la Covid-19 en mars 2020, les autorités européennes ont d'ailleurs particulièrement contrôlé la capacité des CCP à gérer un défaut à distance.

Le CPMI-IOSCO identifie plusieurs points sur lesquels des progrès de la part de l'industrie sont attendus sous deux ans : i) la standardisation de la terminologie et des fichiers d'enchères ; ii) l'implication des membres compensateurs dans la gouvernance ainsi que la participation des clients finaux aux enchères, et sous quelles conditions ; iii) a coordination de stratégies de couverture de portefeuilles du même membre défaillant entre plusieurs CCP.

À la mi-2022, le CPMI-IOSCO évaluera les progrès réalisés et, le cas échéant, pourra émettre des lignes directrices présentant les bonnes pratiques à suivre par les CCP (*guidance*).

1 *A discussion paper on central counterparty default management auctions,* juin 2019.

2 *Central counterparty default management auctions – Issues for consideration et Cover note to the CPMI-IOSCO report on CCP auctions,* juin 2020.

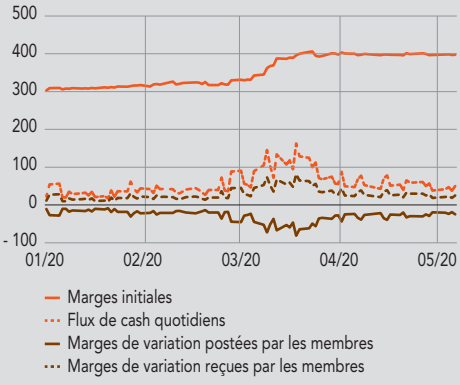
❼ L'impact de la crise liée à la Covid-19 sur l'activité des infrastructures de marché

La crise sanitaire due à la pandémie de Covid-19 a permis d'éprouver la solidité du système financier et la robustesse des réformes mises en place à la suite de la crise financière de 2008.

Les CCP se sont montrées résilientes face aux perturbations des marchés, d'un point de vue aussi bien opérationnel que financier.

À la mi-mars, au plus fort de la crise, les marchés financiers ont connu des niveaux d'extrême volatilité, se traduisant par i) des mouvements de prix parfois supérieurs à ceux qui furent enregistrés en 2008, ii) une forte augmentation des volumes journaliers échangés, et iii) une dégradation de la liquidité sur certains secteurs (comme par exemple sur le marché des actions). Les CCP européennes les plus significatives se sont montrées résilientes dans ce contexte difficile, et ont géré efficacement les risques auxquels elles étaient exposées. Cependant, la forte augmentation de la fréquence et du volume des appels de marge a soulevé des questions plus structurelles sur la pro-cyclicité des marges des CCP, sujet qui continue de faire l'objet d'une attention particulière des régulateurs.

G1 Marges initiales et de variation postées dans les quatre CCP européennes et britanniques les plus importantes (en milliards d'euros)

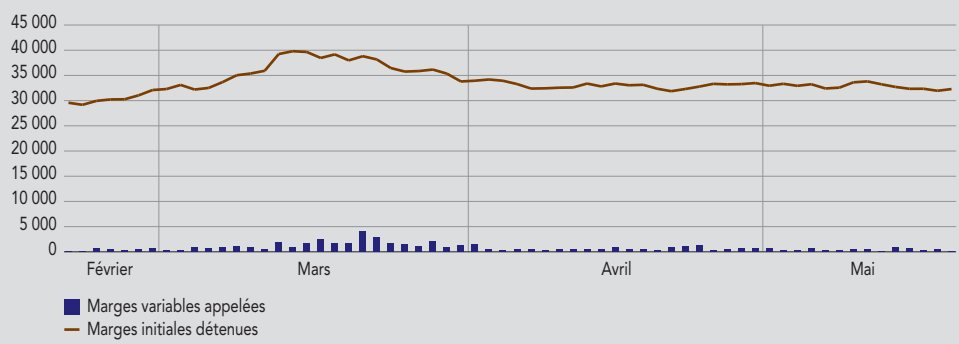


Source : Rapport du Conseil européen du risque systémique, Juin 2020.

Suivant la tendance générale, les volumes compensés en mars par LCH SA ont augmenté sur tous ses segments d'activité. En particulier, les segments EquityClear et CDSClear ont connu des volumes entre deux et trois fois supérieurs aux volumes d'activité normale. Les marges initiales appelées par la CCP ont connu une augmentation de l'ordre de 35 %. Malgré cela, LCH SA a fait preuve de solidité dans la gestion de la crise et la totalité des membres compensateurs a continué à honorer ses obligations envers la CCP.

D'un point de vue opérationnel, l'une des particularités de cette crise est le recours au télétravail généralisé, qui a touché l'ensemble des acteurs des marchés financiers. L'indisponibilité des lieux de travail a demandé aux CCP d'être capables de continuer à opérer à distance de manière effective, se traduisant par la mise en place de plans de contingence et de cellules de gestion de crise, un basculement de plus de 90 % du personnel en travail à distance, le renforcement des systèmes de technologies de l'information (IT) et de communication, ainsi que des systèmes de cyberprotection.

G2 Évolution des marges initiales et de variation de LCH SA (en millions d'euros)



Source : Cartographie 2020 des marchés et des risques, AMF, juillet 2020.

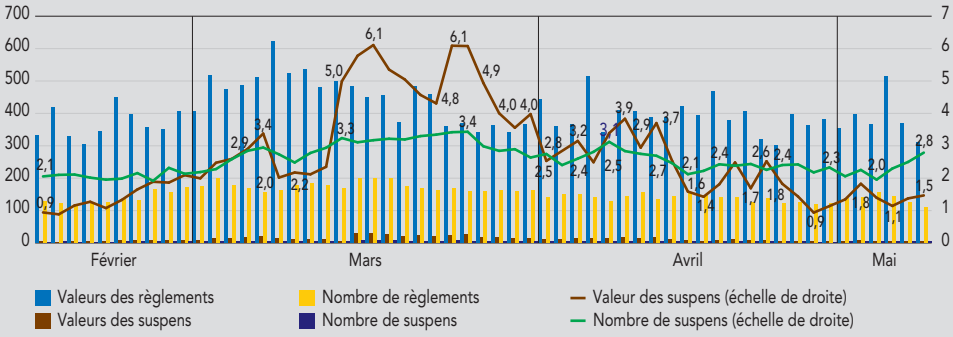
Parallèlement, une attention particulière a été portée par les autorités compétentes aux mécanismes et procédures de gestion des défaillances. Dans ce contexte, LCH SA a conduit plusieurs exercices de *firedrills* depuis le début de la crise, qui ont démontré la capacité opérationnelle de la CCP à pouvoir gérer le défaut potentiel de membres compensateurs à distance.

Les dépositaires centraux de titres ont mis en œuvre avec succès leurs plans de continuité suite à la crise sanitaire de la Covid-19, et ont fait face efficacement à la forte hausse des volumes

Depuis le 16 mars 2020, Euroclear France a imposé le télétravail à plus de 90 % de ses équipes, avec une présence très réduite (uniquement pour certaines fonctions, notamment IT).

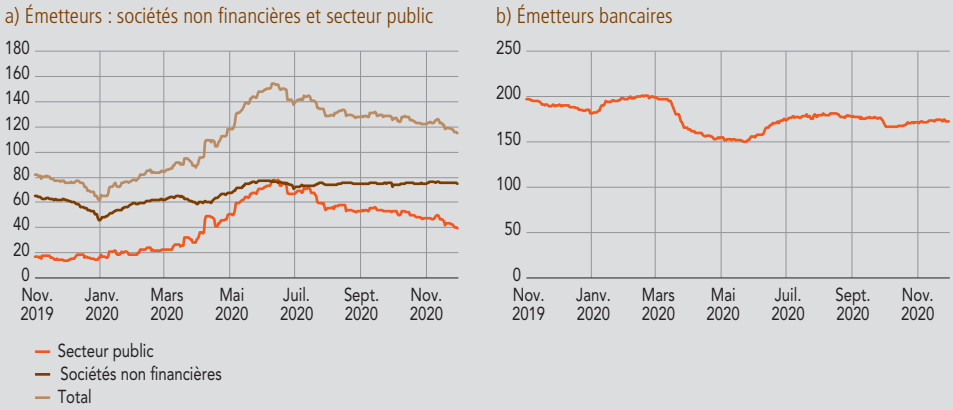
Les premières semaines de la crise de la Covid-19, une forte augmentation du volume et de la valeur des transactions a été constatée par Euroclear France, dont les capacités de traitement ont permis d'absorber ces volumes très élevés. Cette hausse des volumes et l'impact des contraintes liées au confinement des équipes de *back-office* se sont traduits par des taux de suspens en forte hausse, qui ont concerné tous les participants d'Euroclear France. Le volume de transactions et les taux de suspens sont ensuite progressivement revenus à la normale à partir de mi-avril.

G3 Évolution de l'activité sur Euroclear France pendant la crise (échelle de droite en %)



Source : Cartographie 2020 des marchés et des risques, AMF, juillet 2020.

G4 Encours de NEU CP, toutes devises (en milliards d'euros)



Note : Les NEU CP – *Negotiable EUropean Commercial Paper* – sont des titres négociables à court terme.

Source : Banque de France.

ID2S a quant à lui passé tout son personnel en télétravail complet dès le 16 mars 2020. La mise en œuvre du plan de continuité s'est faite sans difficulté opérationnelle. Lors du déconfinement, le télétravail est resté priorisé avec la possibilité pour 50 % des effectifs d'être présents sur site en même temps. Dès l'annonce du second confinement, ID2S est repassé en télétravail à 100 %.

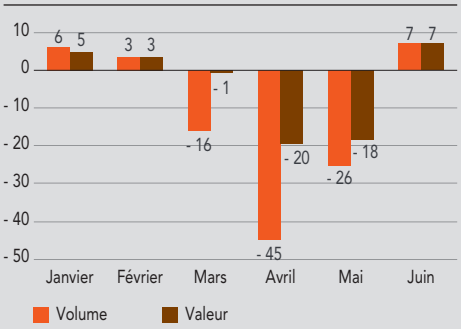
L'évolution positive du marché des NEU CP depuis mai 2020 est principalement due aux émetteurs d'entreprises et aux émetteurs de dette sociale (parmi lesquels la Caisse d'amortissement de la dette sociale).

Les systèmes de paiement français se sont montrés efficaces et résilients lors de la première vague de la pandémie de Covid-19

Au niveau opérationnel, l'opérateur STET a mis à jour son plan de continuite d'activité (PCA) dès le mois de février, pour incorporer les scénarios liés à la Covid-19. Le télétravail s'est généralisé à partir de mi-mars, et a permis un pilotage effectif à distance des activités de STET.

Au niveau du suivi de l'activité, aucun incident ou retard n'a été constaté. S'agissant des flux, une baisse des volumes et valeurs des paiements a été constatée, avec en toile de fond une baisse globale de l'activité économique et de la consommation. Le premier confinement, du 17 mars 2020 au 11 mai 2020, a impacté différemment les instruments de paiement. Ainsi, ce sont les paiements qui nécessitent une intervention expresse du payeur (cartes, retraits DAB, chèques) qui ont connu les plus fortes baisses. Au mois d'avril 2020, les paiement par carte ont subi une baisse de 49 % en volume et de 40 % en valeur (en dépit de l'augmentation de la part du e-commerce par rapport aux commerces classiques), avant d'afficher une augmentation en volume et en valeur pour le mois de juin 2020 par rapport à juin 2019.

G5 Impact du confinement sur les flux échangés dans CORE(FR)
Variation des volumes et des valeurs moyens réglés entre 2019 et 2020 (en %)



Source : STET ; calculs des auteurs

2

LA SURVEILLANCE DES MOYENS DE PAIEMENT SCRIPTURAUX ENTRE 2018 ET 2020

LA SURVEILLANCE DES MOYENS DE PAIEMENT SCRIPTURAUX ENTRE 2018 ET 2020

1 Les évolutions normatives dans le domaine des moyens de paiement scripturaux

1.1 La finalisation du paquet réglementaire lié à la deuxième directive européenne sur les services de paiement (DSP2)

Après l'introduction de l'euro fiduciaire en 2002 et des moyens de paiement SEPA en 2014, l'intégration du marché européen des paiements se poursuit par la voie réglementaire. La première directive européenne sur les services de paiement (DSP1) et les deux directives européennes sur la monnaie électronique (DME1 et DME2), adoptées dans les années 2000, avaient déjà posé les fondements d'un cadre harmonisé en matière de régulation des services de paiement en Europe. Il s'agissait tout à la fois de renforcer la protection du consommateur et d'établir un marché compétitif et innovant. En particulier, depuis leur entrée en application, deux nouvelles catégories d'établissements financiers, les établissements de paiement (EP) et les établissements de monnaie électronique (EME), sont habilités à fournir des services de paiement aux côtés des établissements bancaires. En 2020, 58 établissements actifs avaient été ainsi autorisés comme EP ou EME par l'Autorité de contrôle prudentiel et de résolution (ACPR), après avis de la Banque de France sur la sécurité des services de paiement offerts.

La deuxième directive européenne sur les services de paiement (DSP2), adoptée le 25 novembre 2015, étend le champ de la réglementation européenne à deux nouveaux services de paiement, le service d'information sur les comptes et le service d'initiation de paiement. Ces deux nouveaux services de paiement ont la particularité de ne pas être liés à la tenue d'un compte de paiement et à la manipulation directe des fonds du client. En revanche, ils donnent la capacité aux prestataires de services de paiement (PSP) dûment autorisés d'accéder et d'intervenir à la demande du client sur les comptes ouverts dans un autre établissement. La DSP2 pose, par ailleurs, le principe de l'authentification forte pour les paiements électroniques, en proximité ou à distance, et pour toutes les opérations sensibles susceptibles de constituer un risque de fraude.

Transposée en 2017 en droit français, la DSP2 est entrée en application en janvier 2018, à l'exception des exigences de sécurité précisées par le règlement (UE) n° 2018/389 (RTS Sécurité) qui sont entrées en application après un délai supplémentaire de dix-huit mois en septembre 2019. Ce RTS Sécurité encadre l'accès aux comptes de paiement par les acteurs tiers autorisés à fournir les services d'information sur les comptes et d'initiation de paiement. Il précise notamment les règles de sécurité des interfaces de programmation applicatives, dites API, qui sont construites par les établissements teneurs de compte spécialement pour l'accès des acteurs tiers. Le RTS Sécurité précise également les exigences et les exemptions en matière d'authentification forte du client pour les opérations de paiement électronique et les opérations sensibles.

Plusieurs textes de l'Autorité bancaire européenne (ABE) sont venus compléter la DSP2 pour en préciser les modalités d'application, y compris pour ce qui relève de la sécurité, au titre de laquelle la Banque de France est désignée comme l'autorité compétente en France :

- comme prévu par la directive, l'ABE a adopté trois lignes directrices qui précisent les obligations des prestataires de services de paiement pour la gestion des risques opérationnels et de sécurité (EBA/GL/2017/19) [1], la notification des incidents majeurs (EBA/GL/2017/11) [2] et la déclaration des données relatives à la fraude (EBA/GL/2018/05) [3] ;

1 Ces lignes directrices ont été reprises en 2019 par les orientations sur la gestion des risques liés aux TIC et à la gestion des risques de sécurité (EBA/GL/2019/04).

2 Ces lignes directrices sont en cours de révision par le biais d'une consultation publique lancée le 14 octobre 2020.

3 Ces lignes directrices ont été amendées par de nouvelles orientations en 2020 (EBA/GL/2020/01), qui ont apporté quelques clarifications supplémentaires.

- pour accompagner la mise en œuvre du RTS Sécurité, l'ABE a élaboré des lignes directrices relatives à la procédure d'exemption du mécanisme de secours à l'interface dédiée (EBA/GL/2018/07), ainsi que quatre avis sur la mise en œuvre du RTS Sécurité (EBA-Op-2018-5), l'utilisation des certificats eIDAS (EBA-Op-2018-7), les éléments d'authentification forte (EBA-Op-2019-06) et les entraves à l'exercice des services d'information sur les comptes et d'initiation de paiement (EBA-Op-2020-10). Ce dernier avis identifie les pratiques des établissements gestionnaires de comptes susceptibles de constituer une entrave opérationnelle à la capacité des acteurs tiers à fournir leurs services.

Enfin, la mise en œuvre et l'interprétation du paquet réglementaire de la DSP2 peuvent faire l'objet de questions adressées à l'ABE, dont les réponses sont élaborées en collaboration avec les services de la Commission européenne ainsi que les autorités nationales compétentes comme la Banque de France ou l'ACPR. Au 31 août 2020, 118 réponses relatives à l'application de la DSP2 avaient été publiées par l'ABE [4].

1.2 L'intégration de la DSP2 dans le dispositif de surveillance de la Banque de France

La DSP2 se traduit tout d'abord par de nouvelles exigences statistiques sur l'usage et la fraude aux moyens de paiement. À partir de 2021, les exigences de l'ABE pour la déclaration des données relatives à la fraude (EBA/GL/2018/05) seront notamment intégrées aux collectes de la Banque de France « Cartographie des moyens de paiement » et « Recensement de la fraude aux moyens de paiement », qui deviendront à cette occasion semestrielles. L'ensemble des prestataires de services de paiement PSP établis en France sont assujettis à ces collectes statistiques. Les calendriers, les guides de remplissage et les modalités de remise sont accessibles sur le site internet de la Banque de France [5].

Aussi le canevas de l'annexe au rapport de contrôle interne sur la sécurité des moyens de paiement, qui est exigé par l'article 262 de l'arrêté du 3 novembre 2014 relatif au contrôle interne des établissements financiers, a-t-il été révisé en 2019 pour couvrir les enjeux liés à la sécurité de l'accès aux comptes de paiement et à leurs informations, et pour intégrer le rapport d'audit devant être établi par les PSP sur la mise en œuvre du RTS Sécurité. Ce canevas est accessible sur le site internet de l'ACPR.

Enfin, en application des textes transposant la DSP2, il est prévu que les PSP notifient à la Banque de France la survenance des événements suivants :

- le blocage de l'accès d'un PSP tiers en raison d'un accès non autorisé ou frauduleux [6] ;
- le non-remboursement immédiat d'une opération de paiement non autorisée, lorsque le PSP soupçonne une fraude de l'utilisateur [7] ;
- les incidents majeurs de sécurité [8].

1.3 Le plan de migration de l'OSMP pour l'authentification forte sur les paiements en ligne

Les exigences de sécurité de la DSP2 visent à garantir un niveau de sécurité élevé pour les paiements électroniques en ligne, grâce à la généralisation de l'authentification forte du payeur. Ces mesures de sécurité sont entrées en application le 14 septembre 2019. Toutefois, compte tenu du temps nécessaire à la mise à niveau des protocoles et des systèmes tant chez les banques que chez les commerçants, l'Observatoire de la sécurité des moyens de paiement (OSMP) a défini un plan de migration pour la Place française, conformément à l'avis de l'ABE du 16 octobre 2019 (EBA-Op-2019-11). Ce plan de migration accorde aux acteurs de marché un délai supplémentaire courant jusqu'au 31 décembre 2020 pour se conformer aux exigences d'authentification forte pour les paiements par carte sur internet. Ce plan de migration comprend deux volets :

- un volet à l'attention des consommateurs portant sur l'enrôlement des porteurs de carte dans des dispositifs d'authentification conformes à la définition de l'authentification forte de la DSP2, en remplacement de l'usage du code SMS à usage unique (ou SMS OTP) comme facteur unique d'authentification ;
- un volet à l'attention des acteurs professionnels de la chaîne des paiements, y compris les e-commerçants, portant sur l'évolution des infrastructures d'authentification, notamment du protocole technique 3D Secure, afin d'assurer la gestion des règles de responsabilité et d'exemption à l'authentification forte prévues par la DSP2.

Ces deux volets font l'objet d'indicateurs de suivi assortis de cibles et d'échéances, ainsi que de plans d'action visant à accompagner la mise en conformité de la Place française. Toutefois, le contexte du confinement sanitaire de mi-mars à mi-mai 2020 s'est répercuté sur les trajectoires de migration initialement prévues. Pour en tenir compte, le plan de l'Observatoire a été complété en 2020 pour intégrer une capacité de flexibilité supplémentaire. L'Observatoire a

en même temps décidé d'un certain nombre de mesures complémentaires pour atteindre le plus haut niveau de conformité dans les délais impartis par l'ABE [9] :

- tout d'abord, l'Observatoire a vérifié la disponibilité complète du protocole 3D Secure dans sa version 2 pour les e-commerçants ;

- ensuite, une trajectoire de déploiement du *soft decline* entre septembre 2020 et mars 2021 a été définie pour la Place française. Ce mécanisme permet à l'émetteur de la carte de rejeter une transaction non conforme à la DSP2, tout en permettant au e-commerçant de soumettre une nouvelle fois la transaction via 3D Secure ;

- enfin, l'Observatoire veille à la nécessaire résilience et à la qualité des infrastructures servant à la mise en œuvre de l'authentification forte, dès lors que leur utilisation est appelée à devenir systématique. Un mécanisme de traitement des flux de paiement en cas de défaut de ces infrastructures doit être défini afin d'assurer, dans un cadre normé et commun, l'identification des incidents, le partage d'informations au niveau de la Place et l'activation de modes de traitement alternatifs.

1.4 Le déploiement des interfaces dédiées pour l'accès aux comptes de paiement

Le second volet sécuritaire de la DSP2 porte sur les conditions d'accès aux comptes de paiement par les prestataires tiers autorisés à fournir les services d'information sur les comptes et d'initiation de paiement (ci-après les « acteurs tiers »). En effet, si la DSP2 participe ainsi à l'ouverture des plateformes bancaires (*open banking*), elle vise dans le même temps à préserver la sécurité des données et des opérations bancaires. Depuis l'entrée en application du RTS Sécurité le 14 septembre 2019, les établissements gestionnaires de comptes sont donc tenus de permettre l'accès aux comptes de paiement de leurs clients par les acteurs tiers agréés, sans que cet accès ne puisse être tarifé. Trois modalités d'accès sont possibles pour répondre à cette exigence :

- la fourniture d'un accès via l'interface habituelle de banque en ligne avec authentification de l'acteur tiers (donc sans interface dédiée) ;

- la mise à disposition d'une interface dédiée (API) qui est elle-même dotée d'un mécanisme de secours, reposant généralement sur l'interface de banque en ligne avec authentification de l'acteur tiers ;

- la mise à disposition d'une interface dédiée (API) sans mécanisme de secours, après que l'ACPR a accordé l'exemption de mise en place d'un mécanisme de secours (*voir* infra*, section 2.7*).

La réglementation vise ainsi à mettre fin à la pratique du « *webscrapping* » non authentifié chez les acteurs tiers. Cette pratique consiste à utiliser les données de sécurité personnalisées du client, c'est-à-dire son identifiant et son mot de passe bancaires, pour accéder à son compte de paiement et à ses données. Celle-ci comporte des risques à double titre. D'une part, elle ne permet pas à l'établissement gestionnaire de compte d'identifier les connexions des acteurs tiers. D'autre part, elle oblige le client à partager des données sensibles, qui doivent normalement rester strictement confidentielles.

Afin de soutenir la définition d'un modèle communautaire d'interface dédié (API), la Banque de France et l'ACPR ont créé, en avril 2018, un groupe de travail sur les API promues par la DSP2 rattaché au Comité national des paiements scripturaux (CNPS). Le rôle de ce groupe de travail a été i) d'identifier et de résoudre les points bloquants au déploiement et à l'usage des interfaces dédiées, ii) de relayer et d'expliquer les clarifications apportées au niveau européen, et iii) de partager des indicateurs statistiques sur l'usage des API. Au final, à fin 2020, l'usage des interfaces dédiées pour fournir les services d'information sur les comptes et d'initiation de paiement a sensiblement augmenté. Des améliorations sont toutefois encore attendues au cours de l'année 2021, qui devraient encore augmenter le taux d'utilisation des API et réduire sensiblement la pratique du *webscrapping* non authentifié.

4 Les réponses sont accessibles sur le site Internet de l'ABE : *https://eba.europa.eu/single-rule-book-qa*

5 *www.banque-france.fr/stabilite-financiere/securite-des-moyens-de-paiement-scripturaux*

6 La notification est envoyée à l'adresse suivante : *2323-NOTIFICATIONS-UT@banque-france.fr*

7 Dans le cadre d'une collecte mensuelle à réaliser via le portail de collecte ONEGATE-OSCAMPS.

8 Par le biais d'une interface sécurisée et dédiée, dont les modalités d'accès sont communiquées sur demande envoyée à l'adresse : *2323-NOTIFICATIONS-UT@banque-france.fr*

9 Ces mesures sont détaillées dans le rapport annuel 2019 de l'Observatoire de la sécurité des moyens de paiement. *https://www.banque-france.fr/sites/default/files/medias/documents/820124_osmp2019_web_vf.pdf*

1.5 Les nouvelles recommandations de l'Observatoire de la sécurité des moyens de paiement

La veille sécuritaire est une composante clé de la surveillance des moyens de paiement : elle vise à identifier les risques associés au développement de nouvelles solutions de paiement, de nouvelles technologies ou de nouvelles techniques de fraude, puis à identifier les mesures à même de prévenir la matérialisation de ces risques. En règle générale, cette veille est exercée en coopération avec les acteurs de marché, dans le cadre d'un groupe de travail permanent de l'OSMP, et font l'objet de recommandations publiées dans les rapports annuels de l'Observatoire. Les travaux de veille réalisés dans ce cadre ont en particulier porté sur :

- la sécurité des moyens de paiement SEPA (rapport annuel de l'OSMP de 2017) . Cette étude analyse le fonctionnement du virement et du prélèvement SEPA et identifie les mesures de sécurité appropriées à leurs différents cas d'usage. Les recommandations émises par l'Observatoire portent sur le développement de l'authentification renforcée des opérations, en conformité avec les exigences de la DSP2, le développement d'outils d'évaluation du niveau de risque des transactions, et la sécurisation des données de paiement sensibles dans l'ensemble de la chaine de paiement ;

- la sécurité des modes de paiement non connectés (rapport annuel 2018), c'est-à-dire le chèque, les virements par bordereau et les paiements par carte communiqués sur papier, par courriel ou par téléphone (dits MOTO pour *mail order, telephone order*) : cette étude analyse les risques spécifiques associés à ces pratiques persistantes et rappellent les modalités et les paramètres qui concourent à leur sécurisation. Les recommandations émises par l'Observatoire visent notamment à réduire les faiblesses liées à l'absence d'authentification forte du payeur, et portent ainsi sur la mise en œuvre de dispositifs avancés d'identification de la régularité des transactions à l'initiation et des transactions à risque au moment de leur traitement. L'Observatoire incite également, dans le cadre de la stratégie nationale des paiements portée par le CNPS, au développement de solutions alternatives à ces pratiques, qui sont intrinsèquement plus innovantes et plus sécurisées ;

- la sécurité des paiements par mobile (rapport annuel 2018). Cette étude dressait un panorama et présentait l'état de l'art des solutions de paiement par mobile, avec une attention particulière sur les techniques de traitement des données de paiement sensibles dans ces solutions, comme la tokénisation. Les recommandations émises par l'Observatoire portent sur la protection des données de paiement sensibles par l'ensemble des acteurs impliqués, le développement de l'authentification renforcée – particulièrement pour l'enrôlement des cartes dans les applications de paiement mobile –, la mise en place d'outils d'analyse de risque et la mise en œuvre d'un cadre contractuel protecteur pour les utilisateurs de solutions de paiement par mobile ;

- la sécurité des données de paiement (rapport annuel 2019). Cette étude visait à analyser les nouveaux risques portant sur la sécurité des données de paiement et à identifier les bonnes pratiques permettant d'en assurer la protection tout au long de la chaîne de traitement, chez les utilisateurs, les bénéficiaires et les acteurs de l'industrie du paiement. Les recommandations émises par l'Observatoire portent sur l'application effective dans les conditions fixées par la DSP2 de l'authentification forte des utilisateurs pour l'accès aux services de paiement et à toute donnée sensible, le soutien aux techniques de protection des données sensibles comme le chiffrement et la tokénisation, et le rappel aux utilisateurs des principes de prudence et de confidentialité des données.

1.6 Les cryptoactifs et les *stablecoins* : de nouveaux moyens d'échange qui nécessitent une évolution du cadre réglementaire de surveillance des paiements

En parallèle des moyens de paiement traditionnels, la création du bitcoin en 2008 a donné naissance à une nouvelle catégorie d'actifs, les cryptoactifs, pouvant servir de moyens d'échange. Ces actifs ont pour particularité de combiner deux technologies novatrices qui permettent de sécuriser les transactions, même en l'absence d'un tiers de confiance : i) la chaîne de blocs (*blockchain*), qui lie les transactions de manière irréversible ; et ii) les registres distribués (*distributed ledger technology*, DLT), qui permettent à chaque participant du réseau d'accéder à l'historique de l'ensemble les transactions. L'usage de ces actifs est demeuré très marginal dans le domaine transactionnel, mais la hausse de leur valeur a suscité l'intérêt des médias, l'engouement de certains à des fins d'investissement spéculatif et l'émergence d'un nouvel écosystème entrepreneurial.

Pour novateurs que soient ces actifs, leur usage n'en comporte pas moins des risques que l'expérience a progressivement révélés : au-delà de la possible perte de capital due à leur volatilité, le caractère anonyme des échanges les rend propices aux transactions illicites (blanchiment, financement du terrorisme, évasion fiscale). De plus, en l'absence de protection légale, les utilisateurs sont particulièrement vulnérables aux escroqueries et aux cyberattaques.

Les différentes juridictions ont réagi en ordre dispersé à l'apparition de ces actifs, qui ne correspondaient véritablement à aucune catégorie juridique préexistante. Tandis que certains pays ont tenté d'interdire toute activité en cryptoactifs ou de les assimiler à des catégories juridiques existantes, comme les instruments financiers, d'autres juridictions comme la France ont préféré un cadre légal ad hoc : la loi Pacte a créé en 2018 un nouveau statut de prestataire de services en actifs numériques (PSAN). L'enregistrement comme PSAN est obligatoire auprès de l'AMF dès lors que le prestataire fournit des services de conservation ou d'achat-vente d'actifs numériques en monnaie ayant cours légal. Avant de se prononcer sur la demande d'enregistrement, l'AMF sollicite l'avis conforme de l'ACPR sur le respect de la réglementation relative à la lutte contre le blanchiment et le financement du terrorisme. Pour les autres services sur actifs numériques reconnus par la loi Pacte, l'agrément auprès de l'AMF reste optionnel. Pour autant, au regard du caractère naturellement international de ces activités, une convergence – ou tout au moins, une forme de coopération approfondie – entre juridictions reste nécessaire. Dès 2014, le Groupe d'action financière (Gafi) a réalisé une étude consacrée aux risques de blanchiment et de financement du terrorisme associés aux cryptoactifs [10], avant de modifier, en 2019, ses recommandations pour encadrer spécifiquement ces actifs.

Les questionnements sur la nature de ces actifs et le rôle afférent des banques centrales ont pris une nouvelle dimension à la suite de l'annonce par Facebook du projet Libra en 2018 qui a été renommé Diem fin 2020. Cet événement a été accueilli avec circonspection au regard de l'influence croissante des sociétés technologiques ou Big Tech dans l'industrie des paiements, mais surtout au regard de son effet potentiellement disruptif. En effet, selon ses concepteurs, Diem (ex-Libra) serait en mesure de dépasser la principale limite des crypto-actifs de première génération, à savoir l'instabilité de leur valorisation, grâce à son indexation sur un panier de devises ayant cours légal – d'où le qualificatif de *stablecoin*. Contrairement aux crypto-actifs décentralisés, le Libra serait ainsi émis par une entité centrale, qui prendrait en charge son indexation. Le réseau ambitionne aussi de contourner les infrastructures de paiement classiques afin de pallier certaines insuffisances, notamment dans le domaine des paiements transfrontaliers.

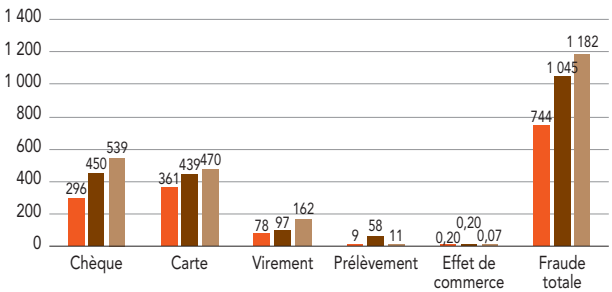
Face à cet enjeu, le G7 a analysé l'impact potentiel de l'émergence de réseaux mondiaux de *stablecoins*. Son rapport, publié en octobre 2019 sous la présidence française, met en exergue les risques induits (en matière notamment de stabilité financière, de protection de la clientèle ou de respect des dispositions LCB-FT [11]) et appelle à une réponse internationale coordonnée, préalable à tout lancement de *stablecoin*. Tel a été l'objet de travaux initiés en parallèle dans le cadre du FSB et qui ont donné lieu à la publication, au mois d'octobre 2020, d'un rapport proposant une adaptation tant réglementaire qu'en matière de surveillance ; c'est également dans ce contexte que la Commission européenne a publié, en septembre 2020, un projet de règlement européen dédié aux crypto-actifs appelé *Market in Crypto-assets* (MiCA).

2 Le bilan de la surveillance des moyens de paiement scripturaux

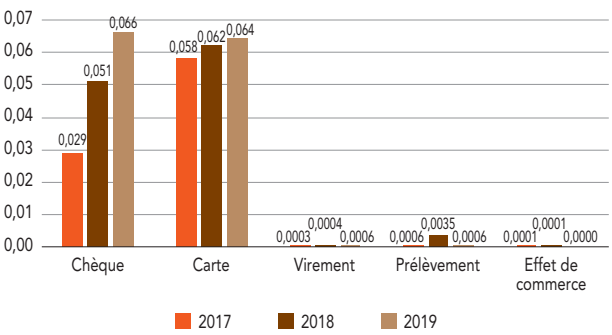
2.1 Bilan triennal sur l'évolution de la fraude aux moyens de paiement [12]

G5 Évolution de la fraude aux moyens de paiement, de 2017 à 2019

a) Évolution de la fraude (en millions d'euros)



b) Évolution du taux de fraude (en %)



Source : Banque de France, Observatoire de la sécurité des moyens de paiement.

10 Gafi, « Monnaies virtuelles : définitions clés et risques potentiels en matière de LCB/FT », 2014.

11 Lutte contre le blanchiment de capitaux et le financement du terrorisme (en anglais *Anti-Money Laundering/Combating the Financing of Terrorism* – AML-CFT)

12 Les données annuelles et détaillées sur la fraude au moyen de paiement sont disponibles via les rapports annuels de l'Observatoire de la sécurité des moyens de paiement accessible au lien suivant : *www.banque-france.fr/liste-chronologique/rapports-dactivite*

De 2016 à 2019, dans un contexte de croissance rapide des flux de paiement, la fraude aux moyens de paiement scripturaux a progressé de manière continue avec toutefois des évolutions contrastées selon les différents instruments de paiement. Le chèque est le moyen de paiement qui a été le plus touché par la fraude sur cette période en devenant depuis 2018 le moyen de paiement le plus fraudé alors même que son usage décroit régulièrement, avec un nombre de chèques émis divisé par près de 2,5 depuis 2004 et une baisse qui se poursuit sur la période récente (1,6 milliard de chèque émis en 2019 contre 1,9 milliard en 2017, soit une baisse de 18 % sur cette période). La part du chèque dans le montant global de fraude aux paiements scripturaux progresse régulièrement pour atteindre 46 % en 2019 avec un taux de fraude à 0,066 %, soit un niveau supérieur à celui de la carte pour une utilisation pourtant beaucoup moins intensive : seulement 6 % du nombre de transactions scripturales se font par chèque, contre 60 % avec la carte.

- En cumulant les transactions de paiement et de retrait, la carte connait également une croissance continue de ses montants fraudés en lien toutefois avec l'augmentation régulière de ses flux puisqu'elle est utilisée dans plus de la moitié des paiements scripturaux (60 % en 2019 contre 58 % en 2017). En conséquence, son taux de fraude reste relativement stable puisqu'il s'établit à 0,064 % en 2019 (contre 0,058 % en 2017). Au niveau national, la fraude n'a progressé que très légèrement sur la période 2017-2019 (0,040 % en 2019 et 0,037 % en 2017). Selon les différents types de transaction effectués en France, la fraude a peu évolué sur la période 2017-2019 sur les paiements en point de vente (0,010 % en 2019), les paiements sans contact (0,019 % en 2019) et les retraits aux distributeurs (0,028 % en 2019). La fraude est beaucoup plus élevée sur les paiements à distance avec toutefois un taux de fraude en baisse continue depuis 2012 et qui s'établit à 0,170 % en 2019 (contre 0,190 % en 2017). S'agissant des transactions internationales [13], elles demeurent toujours plus exposées à la fraude, avec un taux de fraude près de sept fois supérieur à celui des transactions nationales, mais là aussi en amélioration sur la période (0,262 % en 2019 contre 0,281 % en 2017). La fraude sur les transactions internationales présente deux caractéristiques principales : d'une part, elle est concentrée sur les paiements à distance qui représentent plus de 80 % du montant de la fraude et d'autre part, elle est toujours mieux maîtrisée au sein de l'espace européen SEPA qu'en-dehors du fait du renforcement progressif des réglementations européennes concernant la sécurité des paiements (mise en œuvre de la DSP2).

- **Les virements** enregistrent des montants de fraude en progression sur la période 2017-2019 mais sans incidence sur le taux de fraude qui reste à des niveaux extrêmement bas (0,0006 % en 2019) sous l'effet de la croissance continue des flux de paiement et du poids en valeur des virements de gros montant (ceux-ci représentant 46 % des montants échangés par virement en 2019). Cette hausse de la fraude résulte principalement de la recrudescence de faux ordres de virement initiés par des fraudeurs à partir de l'usurpation des données personnelles de connexion aux espaces de banque en ligne ou mobile du client légitime. En 2019, ce canal d'initiation représente à lui seul 55 % de fraude totale sur le virement et un taux de fraude qui s'établit à 0,0023 %, soit à un niveau quatre fois supérieur à celui de ce moyen de paiement à celui de ce moyen de paiement tous canaux confondus.

- Le **prélèvement** est le moyen de paiement qui présente le montant annuel de fraude le plus limité parmi les instruments de paiement accessibles aux particuliers avec des taux de fraude sur la période 2017-2019 extrêmement bas (0,0006 % en 2019). La fraude sur le prélèvement est presque exclusivement nationale (96 % de la fraude totale en 2019), en dépit du caractère européen du prélèvement SEPA.

- Les **effets de commerce** (lettres de change et billets à ordre) restent relativement épargnés par la fraude avec des taux de fraude parmi les plus faibles sur la période 2017-2019.

2.2 L'évaluation de la sécurité au moment des autorisations des établissements de paiement et de monnaie électronique

Dans le cadre de l'instruction des dossiers de demande d'agrément, l'ACPR consulte la Banque de France, au titre de l'article L. 141-4 du Code monétaire et financier, sur les moyens techniques, informatiques et organisationnels relatifs à la sécurité des moyens de paiement. Cette consultation aboutit à la préparation d'un avis de la Banque de France. Entre le 1er janvier 2018 et le 30 septembre 2020, la Banque de France a ainsi délivré à l'ACPR 70 avis positifs, le cas échéant avec certaines conditions suspensives, portant sur :

- 40 procédures d'agrément comme établissement de paiement ou établissement de monnaie électronique ou d'enregistrement comme prestataire de services d'information sur les comptes.

- 12 procédures d'extension d'agrément à d'autres services de paiement portant sur des établissements de paiement ou des établissements de monnaie électronique.

- 18 procédures d'exemption d'agrément au statut d'établissement de paiement ou au statut d'établissement de monnaie électronique, en raison de l'éventail limité de biens et services pouvant être acquis par les moyens de paiement offerts ou du réseau limité de personnes les acceptant.

À l'exception des établissements exemptés d'agrément, ces établissements restent ensuite assujettis à la surveillance permanente de la Banque de France, comme tout prestataire de services de paiement (PSP) opérant en France [14]. Plus particulièrement, ces PSP doivent répondre à l'ensemble des obligations déclaratives auprès de la Banque de France, en matière de statistiques de fraude mais également de description des évolutions de leurs dispositifs de gestion des risques. Ils peuvent aussi faire l'objet de contrôles sur place.

2.3 Le bilan des actions de surveillance sur les émetteurs de moyens de paiement

Au-delà de l'étape d'autorisation des prestataires de services de paiement, le dispositif de surveillance des émetteurs de moyens de paiement scripturaux repose sur plusieurs familles d'actions :

- le contrôle sur pièces, c'est-à-dire l'analyse de la documentation et de données statistiques que les établissements doivent transmettre à la Banque de France sur une base périodique ou à la demande ;

- le contrôle sur place, c'est-à-dire la conduite de missions d'audit thématiques auprès des établissements, et potentiellement de leurs sous-traitants ;

- les échanges bilatéraux avec les établissements sous forme d'entretiens, sur une base régulière ou en fonction de l'actualité.

Via ces différentes actions de surveillance, la Banque de France s'attache notamment à évaluer la conformité des émetteurs aux différents référentiels de sécurité émis par la Banque de France ou l'Eurosystème.

Bilan du niveau de conformité des établissements au référentiel de sécurité du chèque

Le référentiel de sécurité du chèque (RSC) décrit les objectifs de sécurité attendus des établissements intervenant dans le traitement des opérations par chèque. Il est complété par un questionnaire d'évaluation qui détaille les modalités de mise en œuvre de ces objectifs de sécurité. Les établissements de crédit sont ainsi tenus d'évaluer annuellement leur niveau de conformité à ces objectifs. Une nouvelle version de ce RSC est entré en application le 1er janvier 2017 et par conséquent les établissements ont transmis leur première évaluation au cours du premier semestre 2018. Les deux premiers exercices du nouveau référentiel ont mis en exergue à la fois un niveau global de conformité satisfaisant et des défaillances sur plusieurs catégories d'objectifs. Les objectifs de sécurité présentant le niveau de conformité le plus faible concernent à la fois la sécurité physique du chèque et sa protection, son acheminement physique au titulaire, la sensibilisation du titulaire aux règles de remplissage, les dispositifs de surveillance des opérations et enfin, la formalisation de la sécurité en matière de gouvernance et d'organisation.

Ces vulnérabilités sont à mettre en relation avec l'évolution de la fraude sur le chèque depuis 2017. Bien que le déclin de l'usage du chèque se poursuive (-10 % en moyenne par an), le taux de fraude de ce moyen de paiement ne cesse de progresser, ce qui en fait le moyen de paiement le plus fraudé sur deux années consécutives (données 2018 et 2019). Dans ces conditions, afin de lutter contre cette tendance, l'Observatoire de la sécurité des moyens de paiement a inscrit à son programme de travail 2019-2020 des travaux spécifiques de lutte contre la fraude au chèque. Ces derniers sont conduits avec l'ensemble des acteurs de la chaîne de traitement du chèque, en vue de proposer un ensemble d'actions complémentaires visant à renforcer sa sécurité tout en respectant son particularisme lié à sa forme papier et à soutenir la vigilance des utilisateurs, émetteurs et bénéficiaires.

Bilan des missions de contrôle sur place portant sur la qualité des déclarations statistiques

La collecte de données statistiques relatives à l'usage des moyens de paiement et à la fraude est une composante essentielle de la mission de surveillance de la Banque de France, qui lui permet à la fois d'orienter son action et d'en mesurer le résultat. C'est pourquoi les missions de contrôle sur place conduites à l'automne 2017 auprès de quatre groupes bancaires, visaient à évaluer la conformité des processus et de déclaration aux collectes de la Banque de France « Cartographie des moyens de paiement » et « Recensement de la fraude aux moyens de paiement ». Les recommandations formulées à l'issue de ces missions ont porté sur deux aspects :

13 Transactions effectuées par des porteurs français à l'étranger ainsi que celles réalisées par des porteurs étrangers en France.

14 Voir Rapport de surveillance 2014, paragraphe 4.1.2

- d'un côté, l'identification de manquements ou d'anomalies dans les pratiques des établissements audités en matière d'organisation, de pilotage, de processus, d'outils, de contrôle ou de qualité des déclarations statistiques. Des recommandations ont ainsi été adressées aux établissements concernées, pour faire l'objet d'un plan d'action et d'un suivi par les équipes de surveillance de la Banque de France ;

- de l'autre, le recensement des points de méthodologie pouvant donner lieu à interprétation, et qui ont amené la Banque de France à affiner et clarifier ses exigences en matière de déclaration statistique vis-à-vis des établissements assujettis. Les points ainsi identifiés ont été incorporés à la feuille de route de la Banque de France en matière d'évolution des collectes statistiques sur les paiements, et ont alimenté les travaux européens en la matière au moment de la négociation des lignes directrices de l'ABE sur les données de fraude (EBA/GL/2018/05) et au moment de la révision du règlement de la BCE concernant les statistiques relatives aux paiements (BCE/2013/43).

Bilan des missions de contrôle sur place portant sur les dispositifs de sécurisation des paiements des néobanques

La Banque de France avait constaté que le développement, parfois très rapide, de l'activité des nouveaux établissements teneurs de compte (ou néobanques) pouvait créer un effet d'aubaine pour les fraudeurs, qui utilisent notamment ce type de compte comme destination première de transactions frauduleuses visant d'autres établissements avant le transfert des fonds à l'étranger. La persistance d'alertes régulières sur ce sujet a motivé la conduite de missions de contrôle sur place afin d'évaluer la qualité des dispositifs mis en place par les principales néobanques actives sur le marché français. Cette mission a été conduite dans le courant de l'année 2018, auprès de quatre établissements agréés en France comme prestataires de services de paiement.

Il est ressorti de ces missions que, au-delà de la diversité de leur modèle d'activité et de leur profil de risque, les établissements audités pouvaient encore renforcer leur dispositif de pilotage et de maitrise du risque de fraude. En particulier, ces établissements ont fait l'objet de recommandations, formulées en 2019, visant :

- une meilleure structuration de leurs dispositifs internes de lutte contre la fraude en améliorant leur processus de recensement statistique des cas de fraude et en répercutant leurs exigences de sécurité auprès de leurs prestataires et agents ;

- un renforcement de la connaissance de leur clientèle et le développement d'outils de surveillance plus perfectionnés pour mieux détecter et prévenir les opérations frauduleuses ;

- l'engagement de chantiers significatifs de mise à niveau (solutions d'authentification forte à l'émission, compatibilité des infrastructures au protocole 3D Secure dans sa version 2) dans la perspective des nouvelles exigences d'authentification forte prévues par la DSP2 compte tenu des nouvelles exigences d'authentification forte de la DSP2.

2.4 La surveillance des titres spéciaux de paiement dématérialisés et du chèque emploi service universel

En plus de sa mission de surveillance sur la sécurité des moyens de paiement traditionnels, la Banque de France est également en charge, depuis la loi n°2013-100 du 28 janvier 2013, de la sécurité des titres spéciaux de paiement dématérialisés (ci-après TSPD) et de la pertinence des principes de sécurité applicables en la matière. La liste des TSPD est fixée par l'arrêté du 17 juin 2013 et comprend principalement le chèque emploi-service universel préfinancé (ci-après CESU), le titre-restaurant, le chèque-vacances, le chèque-culture et les titres-cadeaux. Cette mission de surveillance des TSPD vient compléter celle exercée par la Banque de France sur le format papier du chèque emploi-service universel inscrite dans le Code du travail (articles R1271-10 et R1271-15) : ces textes prévoient que l'émetteur de CESU est habilité après avis de la Banque de France et s'engage à répondre aux objectifs de sécurité définis par la Banque de France.

Le dispositif de surveillance de la Banque de France s'appuie sur le référentiel sur la sécurité des chèques emploi-service universels et celui sur la sécurité des titres spéciaux de paiement dématérialisés, tous deux publiés en 2015. La surveillance s'exerce concrètement au moyen du questionnaire triennal d'auto-évaluation de la conformité aux référentiels de la Banque de France remis par les émetteurs et de statistiques opérationnels de fraude collectées auprès des mêmes émetteurs. Des entretiens bilatéraux sont par ailleurs menés avec les principaux émetteurs de TSPD et de CESU.

Le niveau de conformité aux objectifs de sécurité des référentiels TSPD et CESU reste globalement satisfaisant, mais un évènement de fraude très significatif sur des CESU papier a fait exploser le taux de fraude sur les CESU en 2019 (0,09 % soit un taux de fraude supérieur au chèque et à la carte). En revanche, le taux de fraude reste extrêmement bas

sur les TSPD. Au global, le montant total de fraude sur les TSDP et les CESU atteint 695 K€ en 2019. Une incertitude demeure toutefois au niveau de la méthodologie de recensement de la fraude chez certains émetteurs. En effet, en cas de perte ou de vol des cartes de titres restaurant, certains porteurs se contentent de faire opposition sur leurs cartes sans contester les opérations non autorisées, ce qui pourrait empêcher les émetteurs d'avoir une vision exhaustive de la fraude. Toutefois, la sécurité des TSPD et des CESU bénéficie de leur dématérialisation croissante qui permet de déployer des dispositifs d'authentification forte, de blocage et d'alertes en temps réel.

De fait, si cette activité reste un marché de niche (2,2 milliards d'euros de transaction en 2019), la dématérialisation de ces titres s'accélère, notamment via le développement de cartes à puce pour les titres-restaurant et l'arrivée de nouveaux émetteurs qui suscitent une nouvelle concurrence. En 2019, les TSPD ont en effet connu une forte croissance avec 143 millions de transactions (+ 49 % par rapport à 2018) pour un montant total de 1,47 milliards d'euros (+ 47 %). Les émetteurs interrogés confirment que la crise sanitaire devrait accélérer la demande des entreprises pour des offres dématérialisées en substitution des offres papier. En 2021, l'Agence nationale des chèques-vacances (ANCV) devrait aussi lancer une première offre dématérialisée et entrerait ainsi dans le périmètre de surveillance des TSPD. En revanche, la dématérialisation stagne pour les CESU. En 2019, dans un marché relativement stable (777 millions d'euros en croissance de + 4,2 %), la part des titres papier augmente même à 69 % (contre 54 % en 2018).

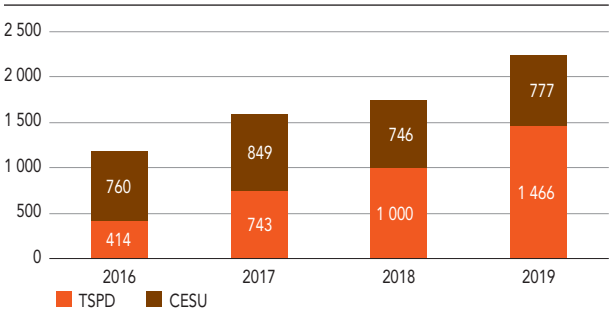
Au cours des prochaines années, le dispositif de surveillance des TSPD et des CESU évoluera à nouveau. En effet, les remises statistiques des émetteurs de TSPD et de CESU qui se font aujourd'hui par courriel en format tableur devront être effectuées via le portail ONEGATE-OSCAMPS. À cette occasion, la collecte statistique deviendra semestrielle tant pour la fraude que pour l'activité, en cohérence avec le dispositif de surveillance des autres moyens de paiement scripturaux.

2.5 La participation de la Banque de France aux actions de surveillance de l'Eurosystème sur les schémas et instruments de paiement

Le cadre de surveillance de l'Eurosystème

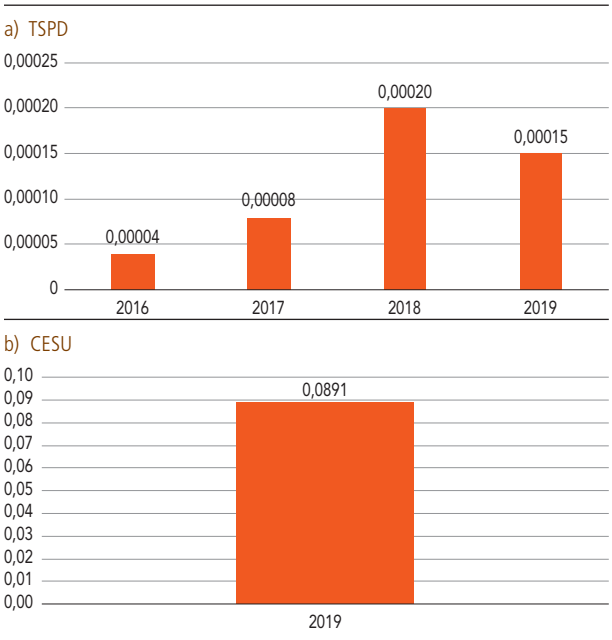
La construction de l'espace unique des paiements en euros confère aux banques centrales nationales une coresponsabilité en matière de sécurité des moyens de paiement. L'Eurosystème a ainsi développé des cadres

G6 Montant des transactions en TSPD et CESU (en millions d'euros)



Source : Banque de France, Observatoire de la sécurité des moyens de paiement.

G7 Taux de fraude (en %)



Source : Banque de France.

de surveillance applicables aux moyens de paiement paneuropéens. En janvier 2008 [15], un premier cadre de surveillance a été élaboré par l'Eurosystème afin d'évaluer la sécurité et l'efficacité des systèmes de paiement par carte (schemes). Les cadres de surveillance relatifs au prélèvement [16] et virement [17] SEPA ont été établis respectivement en août 2009 et en octobre 2010, le Conseil européen des paiements (European Payments Council, EPC) étant l'autorité de gouvernance des instruments SEPA.

Des guides d'évaluations correspondant à chacun de ces trois cadres de surveillance ont également été publiés afin de préciser les attentes de l'Eurosystème. Ceux-ci sont destinés à la fois aux autorités de surveillance et aux autorités de gouvernance des instruments de paiement. Ces guides ont été mis à jour en 2014 et 2015 en incorporant notamment les recommandations sur la sécurité des paiements sur internet publiées par l'Autorité bancaire européenne (ABE) en 2014. À la suite de ces mises à jour, l'Eurosystème a amorcé une nouvelle campagne de surveillance en 2016.

La surveillance des systèmes de paiement par carte (*schemes*)

Pour les systèmes de paiement par carte, les travaux de surveillance ont pris la forme d'un « *gap assessment* », centré sur l'évaluation des nouveaux éléments introduits dans le guide d'évaluation mis à jour en 2015. Le rapport final de l'Eurosystème, publié en 2018, donne un aperçu des évaluations de 16 systèmes de paiement par carte (*schemes*), couvrant 13 *schemes* nationaux et 3 *schemes* internationaux opérant dans la zone euro. La Banque de France a participé très activement à ces travaux de surveillance. Elle a procédé à l'évaluation des 6 *schemes* français (le *scheme* interbancaire Cartes Bancaires et cinq *schemes* privatifs : BNP Paribas Personal Finance, Cofidis, Credit Agricole Consumer Finance, Franfinance et Oney Bank), un nombre record en Europe. Elle a également participé à l'évaluation de trois *schemes* internationaux (Visa, Mastercard, American Express), également très présents en France.

L'exercice a permis de mettre en évidence un degré de conformité élevé des *schemes* français aux exigences du cadre de surveillance, qui a été facilité par les actions conduites dès 2009 par la Banque de France pour renforcer la sécurité des paiements sur internet. Le rapport final de l'Eurosystème, publié en 2018 [18], fait état du large déploiement de solutions d'authentification renforcée par la plupart des *schemes* européens. Parmi les 16 *schemes* européens évalués, 11 *schemes* (dont 5 français) respectaient pleinement tous les standards du cadre de surveillance alors que 5 *schemes* (dont un français) les respectaient d'une manière globale.

Il existait néanmoins des axes d'amélioration en matière de gestion des risques, en particulier dans le domaine de la sécurité, de la fraude et de la continuité d'activité. En conséquence, des recommandations concrètes ont été émises. En 2020, plus aucune recommandation n'était encore ouverte à l'attention des *schemes* français ou internationaux pour lesquels la Banque de France avait procédé ou contribué à l'évaluation. La Banque de France continue de mener des actions de surveillance régulière auprès des *schemes* carte présents sur le territoire national pour évaluer leurs évolutions organisationnelles et techniques et suivre leurs incidents.

Au regard du rôle de plus en plus important de la tokenisation dans le développement des paiements via mobile, l'Eurosystème a également décidé, en 2019, de mener une analyse approfondie sur les activités de tokenisation de Visa Europe et Mastercard Europe. Cette analyse a permis de s'assurer que les niveaux de sécurité associés à la tokenisation sont très élevés. La tokenisation consiste à remplacer une donnée sensible (comme un IBAN ou un PAN) par une donnée de substitution, appelée jeton ou *token*, dans la chaine du paiement. Ce *token* est dédié à une utilisation spécifique et peut être à usage unique ou récurrent. Dans la majorité des cas, la tokenisation permet de stocker un numéro de carte (ou PAN) de manière centralisée et de le communiquer à différentes parties prenantes, sans que ce *token* puisse être détourné pour une autre transaction ou pour un autre mode de paiement. Pour autant, l'essor de la tokenisation a accru la dépendance de l'ensemble de la chaine du paiement aux *schemes* carte internationaux.

La surveillance des systèmes des instruments de paiement SEPA (SDD, SCT et SCT Inst)

L'Eurosystème a également réalisé à partir de 2016 un exercice de surveillance portant sur le prélèvement (*SEPA Direct Debit,* SDD) et les virements SEPA, en décidant pour ces derniers de réaliser concomitamment l'évaluation du virement classique (*SEPA Credit Transfer*, SCT) et du virement instantané (*SEPA Credit Transfer Instantané*, SCT Inst) en raison des similitudes qui les gouvernent. Ces évaluations ont été menées par un groupe de travail constitué de représentants des banques nationales d'Allemagne, d'Espagne, de France, d'Italie, du Luxembourg et de Slovaquie sous la direction de la BCE. Les conclusions ont été entérinées par le Conseil des gouverneurs de la BCE en septembre 2018 et juillet 2019. Dans les faits,

l'exercice d'évaluation se focalise sur l'audit de l'autorité de gouvernance des schemes SEPA, le Conseil européen des paiements (*European Payments Council*, EPC). Le constat est plutôt satisfaisant, mais le rapport appelle l'EPC à renforcer sa gouvernance : tout d'abord, en structurant davantage le suivi et la gestion des risques de fraudes ; ensuite en contrôlant davantage, le cas échéant par échantillonnage, la conformité des participants aux règles des *schemes*.

2.6 La surveillance des interfaces dédiées pour l'accès aux comptes de paiement

Au titre de l'article 521-8 du Code monétaire et financier, la Banque de France s'est vu confier la mission de s'assurer de la sécurité de l'accès aux comptes de paiement et à leurs informations et de la pertinence des normes applicables en la matière. Cette nouvelle compétence est la conséquence de la transposition en droit français de la DSP2 et de l'ouverture de l'accès aux comptes de paiement par les acteurs tiers autorisés à fournir les services d'information sur les comptes et d'initiation de paiement. C'est la raison pour laquelle la Banque de France a publié, en février 2019, le nouveau référentiel de sécurité des interfaces d'accès aux comptes de paiement.

Conformément au RTS Sécurité et à son article 33, l'Autorité de contrôle prudentiel et de résolution peut, après consultation de l'Autorité bancaire européenne, exempter un PSP gestionnaire de comptes de l'obligation de fournir un mécanisme de secours si son interface dédiée présente à la fois un haut niveau de conformité et de disponibilité. En France, cette procédure d'exemption relève de la double responsabilité de l'ACPR, chargée de s'assurer du niveau de performance de l'interface, et de la Banque de France, qui s'assure du respect des exigences sécuritaires. Les exemptions sont formellement accordées par l'ACPR et à ce titre, le secrétariat général de l'ACPR tient le rôle de guichet unique vis-à-vis des établissements et précise la procédure à suivre via un formulaire de demande d'exemption. Dans le cadre de cette procédure, la Banque de France remet un avis sur la sécurité de l'interface dédiée à l'ACPR, qui doit être pris en considération dans la décision d'exemption. Cet avis s'appuie sur une évaluation du niveau de conformité qui doit être conduite par un Centre d'évaluation de la sécurité des technologies de l''information (CESTI) agréé par l'Agence nationale de sécurité des systèmes d'information (ANSSI). À fin 2020, 15 établissements financiers bénéficient en France de l'exemption du mécanisme d'urgence applicables aux API [19].

Par ailleurs, la Banque de France assure une surveillance permanente des API dédiées à l'accès des prestataires tiers. Pour ce faire, elle collecte depuis 2019 des informations additionnelles via l'annexe sur la sécurité des moyens de paiement du rapport annuel sur le contrôle interne (RACI) que doivent remettre annuellement les PSP. Cette annexe doit notamment intégrer les résultats du rapport d'audit que doit annuellement mener l'établissement sur la mise en œuvre du RTS Sécurité (*cf. article 3 du même règlement*).

15 *European central bank, Oversight framework for card payment scheme standards*, janvier 2008.

16 *European central bank, Oversight framework for card payment scheme standards*, janvier 2008.

17 *European central bank, Oversight framework for credit transfer schemes*, octobre 2010.

18 *European central bank, Oversight framework for credit transfer schemes*, octobre 2010.

19 La liste des établissements exemptés de la mise en place d'un mécanisme d'urgence au titre de l'article D.133-10 du Code monétaire et financier est disponible sur le site internet de l'Autorité de contrôle prudentiel et de résolution.

ENCADRÉS

❶

Les travaux du FSB sur l'impact des *stablecoins* et la proposition de règlement européen MiCA

En 2019, le G20 a chargé le Conseil de stabilité financière (*Financial Stability Board* – FSB) d'étudier et de formuler des recommandations pour l'encadrement réglementaire des réseaux de *stablecoins*, en s'attachant particulièrement aux actifs ayant le potentiel d'atteindre une dimension mondiale, les *global stablecoins*. C'est en vertu de ce mandat que le FSB a publié, en octobre 2020, un rapport *Regulation, Supervision and Oversight of Global Stablecoins arrangements*. Le rapport note l'intérêt potentiel des *global stablecoins* en matière d'inclusion financière et d'efficacité des paiements. Il souligne également les risques systémiques sur la stabilité financière que ces réseaux pourraient faire naître, en se substituant pour partie aux devises ayant cours légal dans le domaine transactionnel.

À l'exception de plusieurs pays émergents, le FSB constate que la réglementation existante couvre déjà un pan significatif des activités liées aux *stablecoins*, permettant ainsi de limiter les risques associés à leur développement. Les auteurs du rapport n'excluent pas, cependant, que ces activités évoluent dans le temps, échappant ainsi en partie aux obligations légales. C'est pourquoi une adaptation du cadre réglementaire s'avère nécessaire afin de couvrir l'ensemble des services et infrastructures concernées, et de garantir un traitement réglementaire équitable entre les moyens de paiement traditionnels et ces nouveaux moyens d'échange. Au final, le FSB demande aux porteurs de projet de *global stablecoins* de se conformer avec l'ensemble des réglementations existantes ou en cours de définition, avant le lancement commercial effectif de ces nouvelles solutions.

C'est l'objectif que poursuit la Commission européenne, au niveau européen, via sa proposition de règlement *Market in Crypto-Assets* (MiCA), publiée en septembre 2020 dans le cadre de son plan pour une finance numérique. La Commission souhaite que cette nouvelle réglementation entre en application au plus tard en 2024, dix-huit mois après sa publication au *Journal officiel des communautés européennes*. Outre l'encadrement des services liés aux crypto-actifs de première génération, comme le bitcoin, le projet de règlement prévoit aussi d'encadrer l'émission, la distribution et l'usage des *stablecoins* qui seraient via ce règlement une catégorie particulière de crypto-actifs. Le projet MICA distingue pour ce faire :

- d'une part les « *asset-referenced tokens* », qui sont définis comme un type de crypto-actif adossé soit à plusieurs monnaies ayant cours légal, à des produits comme les matières premières, soit à d'autres crypto-actifs ;

- d'autre part les « *e-money-tokens* », qui sont adossés à une seule monnaie ayant cours légal et dont l'objet est de servir de moyen de paiement, qui sont donc par définition assimilables à de la monnaie électronique. Il est ainsi explicitement prévu par MiCA que les émetteurs de « *e-money tokens* » soient soumis aux règles de la directive monnaie électronique (DME2).

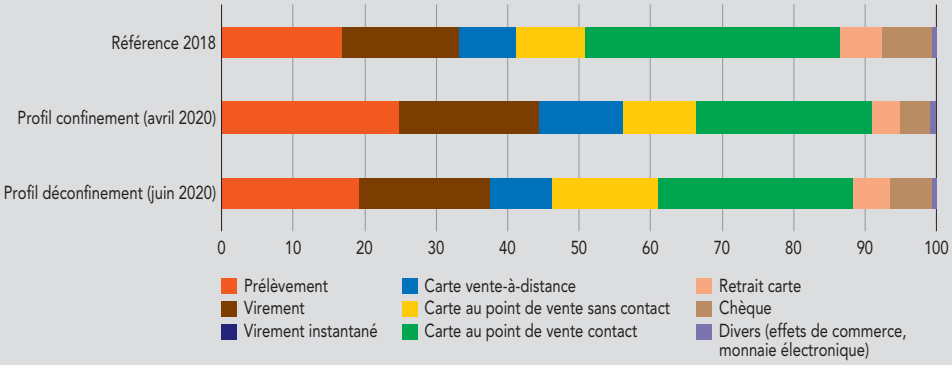
❷ Les moyens de paiement face à la Covid-19 et aux mesures de confinement

Le marché français des paiements s'est montré résilient face à la crise, assurant un traitement efficace et sans discontinuité des flux de transaction. En revanche, des difficultés circonscrites se sont manifestées sur deux moyens de paiement : d'une part, le chèque et notamment les chèques supérieurs à dix mille euros (dits « circulants »), dont le traitement a été affecté par des problèmes de transports ou des capacités temporairement réduites des centres de traitement ; d'autre part le prélèvement interentreprises (dit « SDD B2B »), dans la mesure où les annonces d'allègement de certaines charges professionnelles par les pouvoirs publics ont occasionné des demandes anticipées d'annulation de mandats de prélèvement, entraînant des rejets massifs de prélèvements.

Par ailleurs, le ralentissement de l'activité économique lié à la période de confinement a entrainé une baisse significative des flux de paiement. Les transactions des consommateurs ont été plus affectées que les transactions entre professionnels, traduisant vraisemblablement une plus grande résilience de l'activité des entreprises et des administrations par rapport aux dépenses de consommation. Cette baisse significative des flux de paiement s'est accompagnée d'une évolution des habitudes de paiement : pour des raisons sanitaires, le public et les commerçants ont privilégié autant que possible les moyens de paiement dématérialisés, délaissant les espèces et les chèques au profit des paiements par carte, surtout en sans contact, des paiements mobiles et des paiements à distance sur internet. La part des transactions dématérialisées dans les opérations scripturales est ainsi passée de 50 % avant la crise à 66 % durant le mois d'avril 2020. Cette part était revenue à 61 % en juin durant les premières semaines post-confinement, laissant présager que de nouvelles habitudes ont pu durablement être induites par la crise : c'est par exemple le cas du sans-contact par carte, déjà largement adopté par les utilisateurs, qui est depuis mai 2020 utilisable jusqu'à 50 euros, ou de la baisse encore plus prononcée du chèque dans les commerces.

L'impact de la crise sur le développement de la fraude est encore délicat à appréhender, tant que les déclarations statistiques de fraude ne sont pas effectuées. Toutefois, l'évolution des habitudes de paiement pourrait avoir deux effets opposés : la substitution de la carte ou des moyens de paiement SEPA au chèque pourrait agir favorablement sur le niveau global de fraude ; à l'inverse la croissance des transactions à distance au détriment des transactions de proximité, généralement plus sécurisées, pourrait augmenter le taux de fraude moyen sur la carte. En revanche, les premiers indicateurs indiquent une très bonne maîtrise du taux de fraude sur le paiement sans contact, en dépit de l'augmentation massive de son usage par rapport à 2019 (hausse supérieure à 50 % en volume et à 100 % en valeur à compter de juillet 2020).

Évolution de la part des différents moyens de paiement en nombre d'opérations (en %)



Source : Observatoire de la sécurité des moyens de paiement.

❸ Les quatre piliers de la sécurité des moyens de paiement

L'évaluation de la sécurité des moyens de paiement s'appuie sur la capacité du prestataire à mettre en œuvre quatre piliers complémentaires de prévention, de mesure et de lutte contre la fraude :

1) La sécurité physique et logique

La sécurité des systèmes informatiques dans leur ensemble (systèmes, réseaux, organisation et administration des activités opérationnelles exercées) est examinée sous deux angles, au regard notamment de la protection des données sensibles de paiement : d'une part, la cohérence et la proportionnalité des mesures de sécurité physique des locaux et des centres de données, tels que les contrôles d'accès et la sécurité liée à l'environnement ; d'autre part la cohérence et la proportionnalité des mesures et mécanismes de sécurité logique régissant l'accès interne aux systèmes informatiques, et spécifiant, pour chacune des connexions autorisées de l'extérieur, la nature et la fréquence des contrôles que le prestataire exercera sur ceux-là.

2) L'authentification forte des clients

La sécurité du processus de paiement recouvre deux aspects que le prestataire s'engage à respecter : d'une part, la sécurisation des accès tant à la consultation des comptes qu'aux opérations de paiement par une authentification forte de l'utilisateur ; d'autre part, la garantie faite à l'utilisateur légitime du service de paiement de la mise à disposition et de l'intégrité des facteurs d'authentification, tels que les jetons matériels et les applications mobiles, au moment tant de l'enrôlement initial que du renouvellement.

3) Les outils de détection des opérations à risque (scoring)

Le prestataire doit construire ses systèmes informatiques de manière à analyser les opérations. Cette analyse a pour but de détecter les opérations suspectes ou inhabituelles avant leur exécution et après leur exécution. La Banque de France s'assure du respect par le prestataire de l'existence de ces outils de détection et de leur adéquation à l'activité exercée.

4) La sensibilisation des utilisateurs

Le prestataire doit participer à la sensibilisation des utilisateurs des services de paiement aux règles de vigilance relatives à la sécurité des services de paiement et des outils mis à leur disposition (règles d'accès, problème technique, conservation des identifiants/mots de passe, etc.). La Banque de France s'assure aussi que le prestataire a mis en œuvre une procédure permettant de surveiller, traiter et suivre les réclamations d'utilisateurs liées à la sécurité.

❹

La révision du règlement de la BCE concernant les statistiques relatives aux paiements

La Banque centrale européenne (BCE) a engagé un travail de révision du règlement de 2013 concernant les statistiques relatives aux paiements (BCE/2013/43). La proposition de règlement révisé a fait l'objet d'une consultation publique entre février et mai 2020 et la version définitive a été publiée en décembre 2020 (Règlement (UE) 2020/2011 de la Banque centrale européenne du 1er décembre 2020). Cette révision résulte d'une démarche ambitieuse qui vise à disposer d'un cadre statistique unique répondant aux besoins d'une diversité de métiers : outre la surveillance des moyens de paiement, le nouveau règlement de la BCE doit en effet collecter des statistiques de paiement pour les besoins de la balance des paiements et des prévisions macroéconomiques.

En ce qui concerne la surveillance des moyens de paiement, le règlement révisé de la BCE intègre les exigences statistiques de l'Autorité bancaire européenne au titre de la fraude aux moyens de paiement exprimées dans ses orientations de 2018 (EBA/GL/2018/05). Le règlement révisé de la BCE les complète toutefois à plusieurs titres : tout d'abord, en intégrant une ventilation géographique plus détaillée notamment sur les transactions intervenant au sein de la zone SEPA ; ensuite, en demandant une décomposition des flux et de la fraude par schéma de paiement ; enfin, en demandant pour les opérations transfrontalières par carte à la fois le pays du prestataire de service de paiement de la contrepartie et la localisation du terminal de paiement. Ce nouveau règlement entrera en application en 2022 et il est prévu d'intégrer une partie de ses exigences dans les collectes semestrielles de la Banque de France sur la « Cartographie des moyens de paiements » et le « Recensement de la fraude aux moyens de paiement ».

Ce projet de règlement augmenterait significativement la quantité et la fréquence de données collectées auprès des prestataires de service de paiement. Il devrait aussi fournir des données très utiles pour comparer la sécurité des moyens de paiement au niveau de la zone euro. En effet, jusqu'ici, les seules données de fraude comparables résultent des données de fraude à la carte collectés auprès 23 systèmes de paiement par carte actifs en Europe (ou *schemes* carte). Le sixième rapport de la BCE sur la fraude à la carte a été publié en 2020 sur les données 2018. Les tendances sont globalement cohérentes avec celles observées pour la France par l'Observatoire de la sécurité des moyens de paiement (OSMP). En 2018, le montant de la fraude sur les cartes européennes a été de 1,79 milliard d'euros pour un volume de transaction de 4 780 milliards d'euros, aboutissant à un taux de fraude de 0,038 %. Entre 2014 et 2018, ce taux de fraude a oscillé entre 0,042 % (2015) et 0,035 % (2017). Le léger rebond de 2018, qui avait aussi été observé par l'OSMP, s'explique par la hausse de la fraude sur les paiements à distance (+ 11 %) et sur les paiements de proximité (+ 3,7 %), alors que les retraits étaient moins fraudés (-12,8 %). Comme noté par l'OSMP, la fraude sur les paiements à distance est largement majoritaire (80 % de la fraude) suivie de la fraude aux points de vente (15 %) et aux distributeurs (5 %). Aussi, les transactions internationales sont-elles plus sensibles à la fraude que les transactions au sein de la zone SEPA et les transactions domestiques.

❺ Le futur cadre de surveillance de l'Eurosystème sur les instruments de paiement (PISA)

L'Eurosystème a décidé d'harmoniser les pratiques en matière de surveillance en fusionnant les différents cadres de surveillance existants, qui sont actuellement au nombre de cinq : sur les instruments de paiement (2009), sur les systèmes de monnaie électronique (2003), sur les systèmes de paiement par carte (2008), sur les prélèvements (2010) et sur les virements (2010). Le résultat des concertations au sein de l'Eurosystème a abouti à la proposition d'un cadre de surveillance sur les instruments, les schémas et les dispositifs de paiement (*Eurosystem oversight framework for electronic payment instruments, schemes and arrangements*, PISA). L'objectif de ce cadre PISA est double : i) définir une approche unifiée pour la surveillance des solutions de paiement en appliquant les mêmes principes et les mêmes procédures à toutes les solutions et ii) inclure un certain nombre de nouveaux acteurs dans le périmètre de surveillance à l'instar des solutions digitales ou des portefeuilles électroniques, désignés par le terme « *arrangements* » dans le cadre PISA. En effet, l'innovation dans le domaine des paiements favorise l'émergence de nouveaux modes d'initiation s'appuyant sur une diversité d'instruments de paiement sous-jacents, comme par exemple les solutions de paiement mobile qui s'appuient sur la carte de paiement.

Le projet de cadre PISA a été publié en octobre 2020 pour une procédure de consultation publique ouverte jusqu'au 31 décembre 2020. Ce projet comporte trois documents ayant respectivement pour rôle : i) de fixer le périmètre et les principes (*Oversight framework*), ii) d'identifier les acteurs tombant dans le périmètre de surveillance en fonction de leur importance relative sur le marché européen des paiements (*Exemption policy*) et iii) de préciser la méthodologie de surveillance (*Assessment methodology*). La définition du périmètre de surveillance résulterait d'un système à points fondé sur quatre critères quantitatifs : le nombre d'utilisateurs, le nombre de transactions en volume, le nombre de transactions en valeur et la présence géographique en nombre de pays. Ce système doit permettre de toujours donner la priorité des travaux de surveillance de l'Eurosystème aux solutions de paiement les plus importantes à l'échelle de la zone euro. L'autre innovation de ce cadre PISA serait de couvrir non seulement les paiements en monnaie scripturale mais également d'intégrer les solutions de paiement au moyen d'actifs ou de jetons, qui ne sont pas qualifiés de « fonds » au sens réglementaire, comme les *stablecoins*.

GLOSSAIRE

ABE	Autorité bancaire européenne
AEMF	Autorité européenne des marchés financiers (*European Securities and Markets Authority* – ESMA)
CCP	*Central counterparty* – contrepartie centrale
CFONB	Comité français d'organisation et de normalisation bancaires
CLS	*Continuous Link Settlement* – Système de règlement des transactions de change des États-Unis
CORE(FR)	Système de paiement de détail
CPMI	*Committee on Payments and Market Infrastructures* – Comité sur les paiements et les infrastructures de marché
CPSS	*Committee on Payment and Settlement Systems* – Comité sur les systèmes de paiement et de règlement (devenu le CPMI)
CSD	*Central securities depositories* – dépositaires centraux de titres
CSDR	*Central securities depositories regulation* – règlement européen concernant l'amélioration du règlement de titres dans l'Union européenne et les dépositaires centraux de titres
EMIR	*European market infrastructure regulation* – règlement européen sur les produits dérivés de gré à gré, les contreparties centrales et les référentiels centraux
EPC	*European Payments Council* – Conseil européen des paiements
ESCB-CESR	*European System of Central Banks* (Système européen de banques centrales) et *Committee of European Securities Regulators* (Comité européen des régulateurs pour les valeurs mobilières)
ESES France	*Euroclear Settlement of Euronext-zone Securities France* – Système français de règlement-livraison de titres
EURO1	Système paneuropéen de paiement de montant élevé
FSB	*Financial Stability Board* – Conseil de stabilité financière
IOSCO	*International Organisation of Securities Commissions* – Organisation internationale des commissions de valeurs
LCH SA	Chambre de compensation française
PFMI	*Principles for Financial Market Infrastructures* – principes pour les infrastructures des marchés financiers

Rapport sur la surveillance des moyens de paiement scripturaux et des infrastructures des marchés financiers

Éditeur
Banque de France
39 rue Croix-des-Petits-Champs
75001 Paris

Directeur de la publication
Nathalie Aufauvre
Directrice générale de la Stabilité financière
et des Opérations
Banque de France

Directeur de la rédaction
Valérie Fasquelle
Directrice des Infrastructures, de l'Innovation
et des Paiements

Comité éditorial
Nicolas Péligry, adjoint à la directrice des Infrastructures, de l'Innovation et des Paiements
Pierre Bienvenu, Guillame Bruneau, Véronique Bugaj, Olivier Catau, Bernard Darrius, Florian Dintilhac, Christelle Guiheneuc, Trân Huynh, Julien Lasalle, Alexandra Madeline, Lucas Nozahic, Thomas Piveteau, Mathieu Vileyn (SMPS)
Benjamin Alford, Omar Birouk, Thomas Carré, Alexandre Garcia, Itziar Garcia Bellver, Mathieu Gex, Antoine Lhuissier, Christophe Macé, Claire Orliac, Chloé Terrier et Marie-Aline Vives (SEPI)
Alexandre Capony, Caroline Corcy, Corinne Dauchy (SEL)

Réalisation
Studio Création
Direction de la Communication

Contact
Direction des Statistiques monétaires et financières
Service d'Analyse des financements nationaux
Code courrier : 043-1418
37 rue du Louvre 75002 Paris
Courriel : 1418-CER-UT@banque-france.fr

Impression
Banque de France – SG - DISG

Dépôt légal
Janvier 2021
ISSN en cours

Internet
https://publications.banque-france.fr

Le *Rapport sur la surveillance des moyens de paiement scripturaux et des infrastructures des marchés financiers* est en libre téléchargement sur le site Internet de la Banque de France (*www.banque-france.fr*).

www.banque-france.fr