Rapport

La surveillance des moyens de paiement scripturaux et des infrastructures des marchés financiers

2017

BANQUE DE FRANCE
EUROSYSTÈME

SOMMAIRE

SOMMAIRE

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 les moyens de paiement. Le rapport précédent datait de 2014. Le présent rapport couvre la période allant de 2015 à 2017.

La surveillance des infrastructures des marchés financiers et des moyens de paiement scripturaux a significativement évolué au cours de la période sous revue sous l'effet d'évolutions du cadre réglementaire mais également de l'apparition de nouveaux enjeux. Il convient à cet égard de souligner en particulier les points suivants :

• *la poursuite de la mutation de l'environnement règlementaire en matière de surveillance des infrastructures des marchés financiers : après une première phase de transposition dans des règlements européens, engagée durant les années 2012-2014 sous l'égide de l'Union européenne (UE), des travaux menés par les comités CPMI*[1] *et IOSCO*[2]*, les dernières années ont été marquées par la première revue des règlements existants par la Commission européenne. Ainsi, le règlement EMIR* (European market infrastructure regulation) *a été révisé dans un premier volet consacré aux obligations de compensation et au reporting, et dans son second volet relatif au dispositif de surveillance des contreparties centrales (CCP) de pays tiers et des CCP de l'UE. Au plan international, les travaux sur le rétablissement et la résolution des CCP ont été un des thèmes majeurs d'attention des autorités compte tenu de l'importance systémique de ces infrastructures ;*

• *l'évaluation des premières conséquences de la décision du Royaume-Uni de sortir de l'UE et de l'Espace économique européen : le futur retrait du Royaume-Uni donne une acuité toute particulière à la révision du dispositif européen de surveillance des CCP de pays tiers. En effet, il induit un changement de statut des CCP britanniques, qui deviendront alors vraisemblablement des CCP de pays tiers, alors même qu'elles compensent plusieurs marchés d'importance systémique pour l'UE. Dans le domaine des moyens de paiement, le principal enjeu concerne le devenir du passeport européen permettant aux établissements britanniques d'opérer en France, puisque près de 400 établissements de paiement (EP) ou établissements de monnaie électronique (EME) agréés au Royaume-Uni agissent en France au titre des régimes prévus dans le cadre du passeport européen (libre prestation de services ou libre établissement) – dans l'autre sens, on dénombre moins de vingt EP et EME français opérant au Royaume-Uni. Cette problématique concerne également les établissements de crédit qui peuvent être autorisés à fournir les mêmes services que les EP et les EME, ainsi que les schémas de cartes de paiement Visa et American Express, dont les activités européennes sont opérées depuis Londres ;*

• *l'importance croissante des risques relatifs à la cybersécurité : alors que l'encadrement réglementaire avait jusque-là porté sur la disponibilité des infrastructures, de nouvelles exigences liées à l'intégrité des données ainsi qu'à la résilience globale des acteurs (systèmes, données, processus et personnes) ont été formalisées au sein de plusieurs enceintes* – Guidance on cyber resilience for market infrastructures *du CPMI-IOSCO, directive* network information security *(NIS) sur la sécurité des réseaux et des systèmes d'information pour l'UE, loi de programmation militaire en France – et promeuvent une approche holistique associant l'ensemble des acteurs du secteur financier ;*

1 *Committee on Payments and Market Infrastructures – https://www.bis.org/cpmi/*

2 *International Organization of Securities Commission – https://www.iosco.org/*

• *la sécurité comme enjeu majeur du développement de moyens de paiement innovants et efficaces, permettant de garantir la confiance dans leur utilisation et leur acceptation : l'Europe disposait depuis 2007 avec la première directive sur les systèmes de paiement (DSP1) d'un cadre juridique harmonisé concernant la prestation de services de paiement autour des moyens de paiement de type carte, virement ou prélèvement. En parallèle, le souhait d'accroitre la concurrence dans le secteur en favorisant de nouveaux entrants, tout en garantissant la protection du consommateur, a conduit à l'adoption, le 25 novembre 2015, de la deuxième directive européenne sur les services de paiement (DSP2) qui étend le champ des services de paiement régulés à de nouveaux services et acteurs, tout en renforçant les exigences sécuritaires applicables aux acteurs du marché des paiements. Ce nouveau cadre réglementaire, notamment en ce qui concerne l'obligation de mise en œuvre de l'authentification forte par les acteurs de marché, s'inscrit dans le sillage des recommandations formulées par la Banque de France en la matière. À l'échelon national, le législateur français, par la loi du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique a élargi le mandat de l'Observatoire de la sécurité des cartes de paiement (OSCP) à l'ensemble des moyens de paiement scripturaux. L'Observatoire de la sécurité des moyens de paiement (OSMP) réalise ainsi les analyses de sécurité indispensables aux travaux conduits par le Comité national des paiements scripturaux (CNPS), en charge de veiller à la mise en œuvre de la stratégie nationale des paiements.*

Le présent rapport s'articule autour de deux chapitres principaux qui présentent la surveillance des infrastructures des marchés financiers (chapitre 1) et des moyens de paiement scripturaux (chapitre 2). Chaque chapitre s'attache tout d'abord à présenter les principales évolutions qui ont affecté depuis 2015 le cadre de surveillance puis à décrire les actions de surveillance conduites par la Banque de France.

La surveillance des infrastructures des marchés financiers entre 2015 et 2017

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 infrastructures 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

La période couverte par le précédent rapport de surveillance (2012-2014) avait été marquée par la déclinaison, dans des règlements européens dédiés à différents types d'infrastructures, des principes pour les infrastructures des marchés financiers (PFMI) [1] définis par les comités CPSS [2] et IOSCO [3] au niveau international en avril 2012 : règlement européen EMIR *(European market infrastructure regulation)* publié en juillet 2012 pour les contreparties centrales (CCP) et les référentiels centraux de données [4], règlement CSDR *(central securities depositories regulation)*, publié en 2014, pour les systèmes de règlement-livraison et les dépositaires centraux de titres et règlement de la Banque centrale européenne (BCE)pour les systèmes de paiement d'importance systémique (SPIS), entré en vigueur en 2014.

Des travaux complémentaires ont été conduits au cours de la période sous revue au niveau international sur le rétablissement et la résolution des CCP. Cette période a également été marquée par la première revue des règlements existants et édictés les années précédentes : le règlement EMIR est en effet en cours de révision, tandis que CSDR a été complété par différents règlements délégués (normes techniques). Le règlement BCE pour les SPIS a pour sa part d'ores et déjà fait l'objet d'une première révision en 2017, pour préciser des exigences existantes ou en établir de nouvelles.

1|1 Le rétablissement et la résolution des contreparties centrales : un cadre international précisé

Le rétablissement d'une infrastructure de marché (cf. glossaire CPMI-IOSCO [5]) 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 liées ou non à une défaillance d'un participant ; la mise en œuvre des mesures de rétablissement incombe aux infrastructures des marchés financiers, 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, et vise à permettre l'allocation des pertes, la cessation ordonnée de l'activité, et au besoin, le transfert de l'activité à une entité relais.

1 *Principles for Financial Market Infrastructures – https://www.bis.org/cpmi/publ/d101a.pdf*

2 Devenu entre-temps le comité CPMI *(Committee on Payments and Market Infrastructures) – https://www.bis.org/cpmi/*

3 *International Organization of Securities Commission – https://www.iosco.org/*

4 Les référentiels centraux de données sont supervisés par l'Autorité européenne des marchés financiers (AEMF).

5 *https://www.bis.org/cpmi/publ/d00b.htm?&selection=156&scope=CPMI&c=a&base=term*
Le rétablissement couvre les actions d'une infrastructure de marchés, conformément à ses règles, procédures et autres accords contractuels *ex ante*, pour remédier à toute perte de crédit non couverte, déficit de liquidité ou insuffisance de capital, résultant d'une défaillance d'un participant ou d'autres causes (faiblesses commerciales, opérationnelles ou autres), y compris des mesures visant à reconstituer toute ressource financière préfinancée épuisée et tout accord de liquidité, afin de maintenir la continuité d'activité de l'infrastructure et de continuer à fournir des services essentiels.

Les travaux internationaux sur le rétablissement et la résolution des infrastructures ont connu une accélération dès fin 2014. En octobre 2014, CPMI et IOSCO ont publié un rapport sur le rétablissement des infrastructures[6]. Dans un souci de cohérence, le Conseil de stabilité financière (*Financial Stability Board* – FSB) a adopté en parallèle des recommandations additionnelles portant sur le cadre de résolution, annexées aux *key attributes of effective resolution regimes*[7] et applicables aux infrastructures de marché, dont les CCP.

Compte tenu du caractère systémique des CCP, et des enjeux financiers spécifiques associés au rétablissement et à la résolution de telles infrastructures, des travaux spécifiques leur ont été consacrés, couvrant les aspects relatifs au rétablissement et à la résolution. Les PFMI, et dans leur sillage, le règlement EMIR, avaient d'ores et déjà permis d'assurer un haut niveau de couverture des risques financiers des CCP, qu'il s'agisse des pertes liées au défaut d'un participant (dont la couverture est assurée par les marges initiales et les contributions aux fonds de défaut), ou d'autres types de pertes (liées aux risques opérationnel, commercial ou d'investissement) couvertes d'abord par les fonds propres des infrastructures. Cependant, dans le cadre de la démarche du FSB[8] visant à étendre les dispositifs de rétablissement et de résolution aux établissements financiers systémiques non bancaires, il a été jugé nécessaire de compléter ces principes par des dispositifs permettant de couvrir tous les scénarios de crises envisageables, même peu plausibles. Ces scénarios vont au-delà des scénarios de pertes extrêmes mais plausibles utilisés dans les *stress tests* et qui permettent de calibrer les ressources préfinancées (marges et contributions aux fonds de défaut) des CCP.

Ainsi, au niveau international, en avril 2015, le plan de travail sur les CCP défini par le FSB et associant le Comité de Bâle pour la supervision bancaire et CPMI-IOSCO[9] a inclus un volet sur le rétablissement et la résolution des CCP pour préciser les principes internationaux. Le FSB a publié le 5 juillet 2017[10] une orientation (cf. encadré 1) préparée par un groupe rassemblant autorités de résolution et superviseurs de CCP. En juillet 2017, les comités CPMI-IOSCO ont mis à jour le rapport sur le rétablissement des infrastructures de marché de 2014[11], publié en même temps que l'orientation définitive du FSB, pour tenir compte des évolutions des discussions internationales.

Au niveau européen, la Commission européenne a publié fin novembre 2016 un projet de règlement sur le rétablissement et la résolution des CCP. Cette proposition vise à décliner les standards internationaux dans le cadre juridique de l'Union européenne (UE). L'objectif du règlement est d'encadrer les mesures prises par les CCP dans le cadre de leurs plans de rétablissement, d'accorder aux autorités de résolution les pouvoirs nécessaires à la résolution d'une CCP non viable et de définir les outils appropriés de résolution de façon à garantir la stabilité financière et le maintien des services critiques de la CCP. Le but est d'éviter de recourir aux deniers publics, si ce n'est en ultime ressort, si l'ensemble des autres outils à disposition pour l'allocation des pertes (appels de fonds, décotes sur les marges de variation, cessation anticipée des contrats, absorption du capital de la CCP, etc.) n'ont pas permis d'absorber la totalité de ces dernières. Les États membres de l'UE devront notamment désigner des autorités de résolution pour les CCP ; celles-ci établiront des collèges de résolution qui seront consultés dans le cadre de l'approbation des plans de rétablissement des CCP et participeront au processus d'adoption des plans de résolution préparés par les autorités nationales de résolution.

Le texte proposé par la Commission européenne – et sur lequel les discussions doivent se poursuivre en 2018 – a développé une approche très semblable à celle soutenue par les autorités françaises.

6 *https://www.bis.org/cpmi/publ/d121.pdf*

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

8 *http://www.fsb.org/*

9 *http://www.fsb.org/wp-content/uploads/Joint-CCP-Workplan-for-2015-For-Publication.pdf*

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

11 *https://www.bis.org/cpmi/publ/d162.pdf*

Encadré 1

La résolution des contreparties centrales
Orientation du *Financial Stability Board* du 5 juillet 2017

L'orientation du *Financial Stability Board* (FSB) a pour objectif d'établir un cadre harmonisé au niveau international, en complétant les *key attributes*, pour faciliter la mise en œuvre d'un régime de résolution pour les contreparties centrales (CCP). L'orientation rappelle qu'une résolution ordonnée est essentielle au maintien de la stabilité financière et à la continuité des services critiques d'une CCP. Pour ce faire, les autorités disposeront d'outils et de pouvoirs qui auront vocation à être intégrés à la fois dans le cadre législatif national et dans le *corpus* de règles contractuelles et de fonctionnement des CCP de chaque juridiction (*i.e.* pouvoirs de résiliation partielle ou totale des contrats, d'allocation forcée des positions ouvertes, ainsi que des pouvoirs d'allocation des pertes).

Pour encadrer l'exercice des pouvoirs de résolution, l'orientation consacre d'une part le principe d'équité dans le partage des pertes, distinguant les situations liées au défaut d'un membre compensateur, et 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 seront amenées à effectuer des évaluations précises des besoins financiers pour mener à bien la résolution (évaluations de résolvabilité).

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, notamment :

- entre les autorités de résolution et de supervision lorsqu'elles sont distinctes pour la mise en place des plans de rétablissement et la détermination des scénarios de crise ;

- la mise en place par l'autorité de résolution de l'État d'origine de *crisis management groups* (CMG) pour les CCP d'importance systémique dans plus d'une juridiction, au sein desquels les autorités concernées développeront et coordonneront les plans de résolution ;

- l'instauration d'un cadre de coopération et de partage d'information entre autorités au sein des CMG par la mise en place d'accords contractuels spécifiques (*cooperation agreement* – CoAg).

Enfin, l'efficacité et l'applicabilité transfrontières des mesures de résolution devront être analysées et évaluées par les autorités au regard des dispositifs contractuels, opérationnels et organisationnels des CCP d'importance systémique.

Le FSB a publié à l'été 2017 un rapport présentant une liste de douze CCP identifiées comme systémiques dans plusieurs juridictions[1], sur la base de critères développés par les comités CPMI-IOSCO, et pour lesquelles un CMG a été ou devrait prochainement être mis en place.

1 *http://www.fsb.org/wp-content/uploads/P050717-3.pdf*

La Banque de France promeut le maintien d'une forte flexibilité dans l'utilisation des outils de résolution afin de pouvoir répondre à des situations par définition considérées comme peu plausibles, donc difficiles à anticiper, mais à l'origine d'enjeux élevés en termes de stabilité financière. La possibilité d'intervention précoce des autorités de résolution en tant que de besoin constitue également un axe important de la position française, développée dans le texte européen. S'agissant des outils de résolution, les règles d'allocation des pertes éventuelles des CCP au-delà du mécanisme d'allocation des pertes prévu par le règlement EMIR ne doivent entraîner pour les participants des CCP que des pertes mesurables et gérables dans une situation de tensions sur les marchés, conformément au rapport CPMI-IOSCO de 2014 sur le rétablissement des infrastructures des marchés financiers. Dans ce contexte, la Banque de France considère qu'il faut écarter certains outils qui pourraient nuire à la stabilité financière. Tel est le cas de la décote sur les marges initiales qui crée une exposition potentiellement illimitée des participants, une contrainte de liquidité forte et une incitation pour les membres non défaillants à sortir de la CCP dès qu'un participant fait défaut. L'allocation forcée des positions, qui pourrait conduire à imposer à certains acteurs de prendre des positions qu'ils ne sont pas capables de gérer, est à écarter également, dans la mesure où elle ne ferait qu'ajouter aux risques financiers d'une résolution.

1|2 Le projet de mise à jour du règlement européen EMIR

Le règlement EMIR a fait l'objet de deux propositions de révision par la Commission européenne, l'une axée sur le volet relatif aux obligations de compensation et au reporting, et ayant comme objectif de favoriser une mise en œuvre proportionnée des exigences réglementaires en la matière, l'autre centrée sur le dispositif de surveillance des CCP de pays tiers et des CCP de l'UE.

Le premier volet, dit « EMIR REFIT » [12] a donné lieu à des propositions, publiées le 4 mai 2017, comportant des allègements en matière d'obligations de compensation et de reporting, notamment pour les contreparties non financières, ainsi que l'institution d'une possibilité de suspension temporaire de l'obligation de compensation. Les discussions sont en voie de finalisation dans la perspective d'une adoption du projet de texte en 2018.

Par ailleurs, le 13 juin 2017, la Commission européenne a publié une proposition de révision du règlement, dit « EMIR 2 » visant à refondre le cadre de supervision des CCP de pays tiers et des CCP de l' UE, en modifiant le règlement fondateur de l'Autorité européenne des marchés financiers (AEMF) et le règlement EMIR, qui réglementent les marchés de dérivés de gré à gré et les CCP.

Le futur retrait du Royaume-Uni de l'UE et le changement de statut des CCP britanniques qui deviendront alors vraisemblablement des CCP de pays tiers, nécessitent une revue du dispositif européen relatif aux CCP de pays tiers, dans la mesure où les CCP britanniques compensent plusieurs marchés d'importance systémique pour l'UE. Le dispositif de reconnaissance des CCP de pays tiers prévu actuellement par EMIR n'est pas adapté dans la mesure où il ne confère aucune marge d'appréciation ni véritable pouvoir de contrôle à l'AEMF, alors même que certaines CCP de pays tiers reconnues ont de fortes interdépendances avec le système financier de l'UE. La Commission propose donc une approche proportionnée, qui permet de définir des exigences différenciées pour les CCP de pays tiers en fonction de leur importance systémique pour l'UE (cf. encadré 2).

Concernant les CCP établies dans l'UE, la compétence de supervision resterait nationale ; un rôle accru de l'AEMF permettrait de favoriser une plus grande convergence des dispositifs de supervision au niveau européen. En outre, les banques centrales d'émission des devises dans lesquelles les CCP compensent des transactions disposeraient également d'un pouvoir plus

12 REFIT : *Regulatory Fitness and Performance Programme.*

Encadré 2

Brexit : impacts sur les infrastructures de marché

La décision du Royaume-Uni de sortir de l'Union européenne (UE) et de l'Espace économique européen (EEE), qui prendra effet en mars 2019, 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. LCH Ltd compense ainsi 95 % du marché mondial des *swaps* de taux, y compris en euro et dans cinq autres devises de l'UE, ainsi qu'environ 30 % du marché du *repo* compensé en euro et ICE Clear Europe Limited compense le LIFFE [1], marché de dérivés listés de taux courts, et a une position majoritaire dans l'UE sur la compensation des *credit default swaps* – CDS.

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 EMIR, qui rassemblent les autorités européennes principalement intéressées, y compris l'Autorité de contrôle prudentiel et de résolution et l'Autorité des marchés financiers au titre de la supervision des adhérents compensateurs français, et la Banque centrale européenne en tant que banque centrale d'émission de l'euro. Après la sortie du Royaume-Uni de l'UE et de l'EEE, ces CCP seront soumises aux règles britanniques et leurs collèges EMIR disparaîtront : elles deviendront des CCP de pays tiers, soumises à un régime d'équivalence qui est actuellement très peu contraignant pour les CCP concernées et leurs superviseurs domestiques.

Afin de pallier ces déficiences, la Commission européenne a publié le 13 juin 2017 une proposition de refonte du dispositif réglementaire de supervision des CCP de pays tiers, qui renforce notamment les pouvoirs de l'Autorité européenne des marchés financiers (AEMF) et des banques centrales d'émission dans le cadre du dispositif de reconnaissance des CCP de pays tiers. Le dispositif proposé proportionnerait le régime de supervision d'une CCP à son importance systémique pour l'UE :

- pour les CCP non systémiques, le dispositif de reconnaissance actuel fondé sur l'équivalence des cadres réglementaires serait maintenu, mais revu régulièrement et assorti de conditions pour assurer la réalité de l'équivalence ;
- pour les CCP d'importance systémique, la conformité stricte aux exigences d'EMIR serait obligatoire et vérifiée par une supervision directe de l'AEMF, ainsi qu'une soumission aux règles imposées par les banques centrales d'émission dans leur domaine de compétences ;
- si certaines activités de compensation sont jugées particulièrement systémiques pour l'UE, un pouvoir de refus de reconnaissance (qui imposerait une relocalisation dans l'UE) est confié à la Commission européenne, sur recommandation de l'AEMF après accord des banques centrales d'émission concernées.

Ces dispositions naissent de plusieurs constats, à la lumière de l'expérience passée :

- une CCP qui effectue des opérations libellées en euros ou dans une autre devise de l'Union européenne mais qui n'est pas principalement contrôlée par une autorité de l'UE 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 ;
- la perspective du Brexit et l'abandon du cadre réglementaire européen pour les CCP britanniques renforcent la nécessité de relocaliser dans l'UE la compensation des instruments libellés en devises de l'UE qui revêtent une importance stratégique pour la mise en œuvre de la politique monétaire, le financement de l'économie et la stabilité financière dans la zone.

La Banque de France soutient donc fortement cette initiative qui donnera aux autorités européennes les moyens de mettre en œuvre leur mandat au service de la stabilité financière de l'UE, en garantissant la conformité des CCP de pays tiers qui veulent fournir des services dans l'Union aux exigences réglementaires européennes.

1 *London International Financial Futures and options Exchanges*

important, et contraignant, de revue des décisions qui les concernent plus directement au titre de leur mandat de mise en œuvre de la politique monétaire.

1|3 La révision du règlement pour les systèmes de paiement d'importance systémique

L'environnement réglementaire des systèmes de paiement a connu des modifications substantielles avec la révision des dispositions du règlement UE n° 795/2014 de la BCE du 3 juillet 2014 concernant les exigences de surveillance applicables aux systèmes de paiement d'importance systémique (SPIS) aboutissant au réglement BCE n° 2014/28. Cette révision est la première depuis la publication du règlement et doit ensuite intervenir tous les deux ans. Elle s'est appuyée sur les enseignements tirés des travaux de surveillance de l'Eurosystème depuis l'adoption du règlement précité en 2014, et de la consultation des opérateurs des quatre SPIS – TARGET2, EURO1, STEP2-T, CORE(FR) – qui s'est tenue entre décembre 2016 et février 2017. Le réglement révisé, publié le 16 novembre 2017[13], apporte des précisions sur les obligations existantes, intègre de nouvelles exigences en matière de gestion des risques et élargit enfin les pouvoirs des autorités.

Ainsi, le règlement révisé renforce le cadre de gouvernance des SPIS, avec l'introduction d'un administrateur indépendant et des précisions sur la séparation claire des fonctions opérationnelles, des fonctions de risques et d'audit interne. Les exigences en termes d'implication et de responsabilité du conseil d'administration sur les décisions ayant un impact sur le profil de risque du système, sont également renforcées.

En matière de risques, le règlement révisé clarifie les exigences associées à la couverture des risques financiers, notamment de liquidité, et complète les obligations relatives à la gestion du risque d'activité. À cet égard, le règlement prévoit la ségrégation des actifs, entre ceux affectés à la couverture du risque d'activité et ceux mis à disposition pour les opérations quotidiennes, mais aussi la distinction entre d'une part, le plan de rétablissement et de fermeture ordonnée du système de paiement et d'autre part, le plan de recapitalisation. Le règlement révisé comporte en outre des dispositions complémentaires sur la gestion des risques de conservation, d'investissement et du risque opérationnel. Sur ce dernier volet, le règlement spécifie des exigences portant sur le cyber-risque, dans le sillage de l'orientation CPMI-IOSCO sur la cyber-résilience des infrastructures de marché (cf. section 1|5). Les opérateurs sont désormais tenus de justifier régulièrement auprès du surveillant le cadre de la gestion du cyber-risque en termes de gouvernance, d'identification, de protection, de détection, de tests et de résilience.

Les opérateurs doivent se conformer à ce nouveau cadre réglementaire dans un délai de dix-huit mois pour les dispositions relatives aux obligations financières, et de douze mois pour l'ensemble des autres dispositions.

Enfin, les autorités compétentes se voient dotées de pouvoirs d'imposition de mesures correctrices, voire de sanctions, pour la BCE. Le règlement révisé s'accompagne également d'une notice méthodologique qui détaille les modalités de calcul des sanctions financières, ainsi que de la modification du règlement BCE n° 2157/1999 relatif aux sanctions.

1|4 La finalisation de la règlementation européenne pour les dépositaires centraux de titres

Le règlement européen n° 909/2014 concernant l'amélioration du règlement de titres dans l'UE et les dépositaires centraux de titres (communément appelé *central securities depositories regulation* – CSD), a été adopté le 23 juillet 2014. Il transpose réglementairement les PFMI applicables à ces infrastructures, tout en les précisant.

Si les PFMI considèrent que les dépositaires centraux de titres (*central securities depositories* – CSD)

13 *http://www.ecb.europa.eu/ecb/legal/pdf/celex_32017r2094_fr_txt.pdf*

n'exploitent pas nécessairement un système de règlement-livraison de titres, CSDR crée en revanche un lien très étroit entre les CSD et les systèmes de règlement-livraison. En effet, sous CSDR, un dépositaire central de titres doit obligatoirement exploiter un système de règlement-livraison pour pouvoir être qualifié de CSD, en plus d'offrir au moins l'un des deux autres services de base définis par CSDR (*i.e.* un service notarial et/ou une tenue centralisée de comptes titres au plus haut niveau) ; dès lors, en Europe, les CSD sont les seules entités autorisées à exploiter un système de règlement-livraison, aux côtés des banques centrales faisant office de CSD.

Des règles prudentielles harmonisées sont désormais applicables pour l'ensemble des risques auxquels les CSD sont exposés (en particulier le risque juridique, le risque opérationnel, etc.). Les cadres de gestion des risques doivent permettre à un CSD d'identifier, de gérer et de maîtriser les risques auxquels il est exposé, y compris sur les activités qui ont été externalisées dont il est précisé qu'elles doivent rester contrôlées par le CSD. Des méthodes de calcul des exigences en fonds propres ont été définies, qui doivent permettre au CSD de couvrir à la fois les risques auxquels il est exposé, mais aussi permettre sa liquidation ou sa restructuration ordonnée sur une période d'au moins six mois. En termes pratiques, cela requiert du CSD de pouvoir assurer le paiement des frais de fonctionnement sur une période d'au moins six mois.

CSDR introduit également des dispositions harmonisées relatives au fonctionnement des marchés de titres, notamment i) la généralisation de la dématérialisation des titres (effective en France depuis 1984) ou de leur immobilisation ; ii) l'harmonisation de la durée du cycle de règlement, désormais de deux jours ouvrés au maximum entre la date de négociation J et la date de règlement J+2 pour les transactions négociées et exécutées sur des plateformes de négociation ; iii) le renforcement des mesures de discipline de marché, qui visent à limiter les occurrences de défaut de livraison de titres et/ou d'espèces – mesures préventives des suspens, et application de pénalités financières en cas de retard du dénouement par rapport à la date de règlement convenue, voire de procédures de rachat forcé de titres *(buy-in)* lorsque le retard excède quatre jours ou sept jours selon les titres.

Enfin, CSDR a pour ambition de décloisonner le fonctionnement du post-marché en Europe, qui s'articule encore autour de « lignes de partage nationales ». Deux mesures importantes doivent concourir à la réalisation de cet objectif. D'une part, les émetteurs doivent pouvoir émettre leurs titres dans le CSD européen de leur choix, et non plus nécessairement dans le CSD national, sous réserve du respect de certaines dispositions du droit de leur pays d'origine. Cette possibilité était ouverte avant l'adoption de CSDR mais très peu utilisée en pratique ; CSDR, en prévoyant explicitement cette possibilité, vise à ouvrir davantage l'activité de « CSD émetteur » à la concurrence entre CSD de l'UE. Ceci devrait leur permettre de sélectionner le ou les CSD les plus à même de gérer leurs titres de façon efficiente. D'autre part, CSDR consacre le principe selon lequel les CCP et les plateformes de négociation doivent fournir à un CSD, à sa demande, un accès transparent et non discriminatoire à leurs flux de transaction, qui peut être soumis à une tarification commerciale raisonnable. Les CCP et plateformes de négociation ne seront plus en mesure de refuser de tels accès, sauf s'ils sont de nature à créer des risques trop importants pour les CCP et plateformes concernés.

Si CSDR est entré officiellement en vigueur le 17 septembre 2014, il n'entre progressivement en application que depuis fin 2017. En effet, certains règlements délégués complétant le règlement par des mesures techniques (en particulier ceux ayant trait aux exigences opérationnelles, d'agrément et de surveillance applicables aux dépositaires centraux de titres) ont été adoptés début 2017 par le Parlement et le Conseil européens, puis publiés au *Journal officiel* de l'UE le 10 mars 2017. En outre, selon les derniers éléments d'information

disponibles, des mesures spécifiques à la discipline de marché feront l'objet d'une publication de règlements délégués complétant CSDR par des mesures techniques d'application début 2018. Ces normes entreront en vigueur deux ans environ après leur publication, ce qui laisse anticiper une application effective début 2020 des mesures de discipline de marché.

La plupart des États européens n'ont désigné qu'une autorité compétente pour l'application de ce règlement ; dans l'immense majorité des cas, il s'agit de l'autorité des marchés financiers ; quelques États ont désigné deux autorités compétentes : c'est le cas de la France, qui a désigné l'Autorité des marchés financiers (AMF) et la Banque de France. L'AMF est compétente pour délivrer l'agrément, sur consultation de la Banque de France. Cette dernière est compétente au premier chef sur certains sujets tels que la finalité des règlements, le règlement espèces, les liens entre CSD, le risque opérationnel ou encore la politique d'investissement. Des « autorités concernées » interviendront également dans le processus d'autorisation, notamment la banque centrale d'émission (l'Eurosystème dans le cas des CSD traitant en euros, qui sera représenté par la banque centrale nationale de la juridiction d'établissement des différents CSD). Elles peuvent émettre des avis à l'autorité compétente/aux autorités compétentes d'un CSD, sur les sujets pertinents de leur point de vue, ces avis n'étant toutefois pas liants.

Dès l'entrée en vigueur de la norme technique (*regulatory technical standard* – RTS) relative à l'agrément, le 30 mars 2017, les dépositaires centraux de titres européens déjà en opérations ont eu un délai de six mois pour soumettre leur dossier d'agrément sous CSDR, ce qui a fixé au 30 septembre 2017 la date limite de soumission des dossiers par les CSD auprès de leur(s) autorité(s) compétente(s). Cela s'applique notamment à Euroclear France, le seul CSD actuellement en opération en France.

Au cours du processus d'agrément, les CSD européens déjà en opérations disposent d'une « clause de grand-père » qui leur permet de continuer à offrir tous les services listés par CSDR, y compris les services de base expressément réservés aux CSD par le règlement européen. Toutefois, si ce processus se conclut par un refus d'agrément, ils devront alors cesser d'offrir les services proposés jusqu'ici, en particulier l'exploitation de leur(s) système(s) de règlement de titres. Un CSD nouvellement créé devra, quant à lui, être agréé sous CSDR avant de pouvoir commencer ses opérations, et en particulier avant d'exploiter un système de règlement de titres.

À compter du dépôt du dossier d'autorisation par les CSD, les autorités compétentes disposent d'un délai de trente jours ouvrés pour évaluer sa complétude. Si le dossier est jugé complet, les autorités compétentes disposent ensuite de six mois non prorogeables pour décider d'agréer ou non le CSD, éventuellement en lui demandant toute information complémentaire qui sera jugée nécessaire à son agrément. En revanche, si le dossier est jugé incomplet, les autorités compétentes doivent le notifier au CSD et déterminer le délai qui lui est accordé pour soumettre les éléments complémentaires.

CSDR prévoit à son article 75 que, d'ici au 18 septembre 2019, la Commission européenne revoit et prépare un rapport sur le règlement CSDR.

1|5 La mise en œuvre de nouveaux principes internationaux dans le domaine de la cyber-résilience

Le bon fonctionnement des infrastructures de marché est une nécessité vitale, compte tenu des liens avec l'économie réelle et du haut niveau d'interconnexion des écosystèmes financiers. L'accès aux données rendu possible depuis des points d'entrée multiples et la vitesse de transmission de l'information et du traitement des données ont fortement contribué à améliorer l'efficacité des infrastructures des marchés financiers, en permettant de réduire les coûts tout en augmentant

les volumes traités. Dans le même temps, cette évolution a elle-même transformé la nature des risques, et la sécurité du système d'information, qui était le paradigme dans les années 2000, a pris une nouvelle dimension pour devenir la cybersécurité dans les années 2010. Avant les années 2000, la « question cyber » était en effet essentiellement appréhendée sous le seul angle de la protection des données. Le champ d'analyse s'est élargi dix ans plus tard pour inclure la détection, l'analyse *ex post*, jusqu'à la résolution des cyberattaques.

La prise de conscience par les différents acteurs du secteur financier des dangers et impacts avérés des cyber-risques, a atteint son apogée en mars 2016 avec l'attaque dont a été victime la Banque centrale du Bangladesh.

Dans ce nouveau contexte, l'approche des cyber-risques par les autorités de surveillance a fortement évolué. Pendant plusieurs années, les efforts réglementaires ont essentiellement visé la disponibilité des infrastructures, puis l'intégrité des données. Désormais, s'ajoute à ces exigences la notion de résilience globale au travers de la préservation des fonctions et données critiques permettant d'effectuer des opérations de compensation, de paiement ou de livraison de titres, dans les délais impartis. Ainsi, la cyber-résilience ne se résume pas à une seule question technologique mais englobe maintenant les systèmes et les données, ainsi que les personnes et les processus.

Les cybermenaces devenant un enjeu de sécurité et de résilience de premier plan pour l'écosystème financier, les pays membres du G7 ont publié en 2016 les *G7 fundamental elements of cybersecurity for the financial sector*[14]. Ce document non prescriptif a servi de point d'ancrage pour le développement harmonisé de stratégies nationales pour l'ensemble du secteur financier, y compris les banques et autres institutions financières. Il décline huit éléments principaux pour la gestion du cyber-risque : stratégie et cadre de gestion du risque, gouvernance, évaluation et contrôle du risque, surveillance continue du risque, réponse à un cyber-incident, recouvrement après un cyber-incident, partage d'informations et apprentissage continu.

Concernant plus particulièrement les infrastructures de marché, le cyber-risque n'était pas traité spécifiquement dans les standards internationaux de surveillance. Il est intégré sans traitement spécifique dans les exigences sur la gestion du risque opérationnel (principe 17 des PFMI publiés en 2012 par CPMI-IOSCO). Les cyberattaques se multipliant et gagnant en sophistication dans les années 2010, et les infrastructures de marché/systèmes de paiement apparaissant comme des vecteurs de contagion rapide au secteur financier, un groupe de travail rassemblant banques centrales, superviseurs financiers et organisations internationales a été mandaté pour élaborer des standards internationaux spécifiques au cyber-risque, complémentaires des PFMI.

Ces travaux, initiés fin 2014, ont abouti courant 2015 à des projets de standards qui ont ensuite été soumis à consultation publique entre novembre 2015 et février 2016. La *Guidance on cyber resilience for market infrastructures*[15] a ensuite été publiée par CPMI-IOSCO fin juin 2016. Ce document sert aujourd'hui de référence aux travaux des infrastructures et de leurs autorités pour accroître la cyber-résilience. La *Guidance* est structurée en cinq thèmes principaux : gouvernance, identification, protection, détection et reprise. Ils sont complétés par des aspects relatifs à la culture et la perception de la situation, la formation ou encore les cybertests (par exemple les tests d'intrusion dans les systèmes), concepts qui n'étaient pas systématiquement abordés dans les standards antérieurs.

Au niveau européen, au terme de trois années de négociation, les travaux engagés par la Commission européenne ont abouti à la publication, le 19 juillet 2016, de la directive sur la sécurité des réseaux et des systèmes d'information, connue sous l'appellation de

14 *G7 fundamental elements of cybersecurity for the financial sector*

15 *Guidance on cyber resilience for market infrastructures*

directive NIS *(Network Information Security)*. Les États membres doivent transposer dans leur législation nationale cette directive d'ici mai 2018.

En France, des exigences spécifiques avaient été publiées de façon anticipée dès 2013 pour le secteur financier dans le cadre de la déclinaison de la loi de programmation militaire[16], dont le respect est vérifié par l'Agence nationale pour la sécurité des systèmes d'information (ANSSI).

La publication de la *Guidance on cyber resilience for market infrastructures* et l'occurrence d'une cyberattaque majeure dans le système financier ont rendu prioritaire, tant pour les surveillants que pour les opérateurs d'infrastructures, l'amélioration globale du niveau de cyber-résilience du secteur visant à réduire l'effet de « maillon faible » ou l'impact général d'un incident.

L'Eurosystème s'appuie sur la CPMI-IOSCO *Guidance* pour mener un travail d'évaluation de la cyber-résilience des systèmes de paiement et infrastructures de marché européens, en vue de son renforcement. Les travaux sont déclinés autour de deux axes :

- favoriser le dialogue entre régulateurs et industrie : l'*European Cyber Resilience Board* est un forum stratégique de haut niveau (*strategic high level meeting*) entre régulateurs et industrie au sujet de la cyber-résilience des infrastructures de marché et des fournisseurs de services critiques. L'objectif de ce forum est d'introduire une interface de dialogue, d'élever le niveau de conscience sur le sujet de la cybersécurité pour les régulateurs et les assujettis, et de renforcer et favoriser les initiatives conjointes visant à améliorer la cyber-résilience du secteur ;

- créer un cadre harmonisé pour la réalisation de tests d'intrusion de type *red-teaming* : les travaux lancés début 2017 aboutiront à la publication de guides à l'usage des autorités autant que des opérateurs et des sociétés spécialisées auxquels elles feront appel pour mener ces opérations délicates.

16 *https://www.legifrance.gouv.fr*

2| Le bilan de la surveillance des infrastructures des marchés financiers

En tant qu'autorité nationale, la Banque de France assure, aux côtés de l'ACPR et de l'AMF, selon les infrastructures concernées, la surveillance des infrastructures des marchés financiers opérant en France : la chambre de compensation LCH SA, le dépositaire central de titres Euroclear France et les systèmes de paiement français CORE(FR) et paneuropéen SEPA.EU. Elle participe également à la surveillance coopérative de plusieurs systèmes de paiement, infrastructures de marché et fournisseurs de services critiques établis dans d'autres pays et/ou de dimension paneuropéenne voire internationale.

2|1 LCH SA

Activité

Depuis le 11 avril 2016, la chambre de compensation française porte le nom commercial de LCH SA (anciennement LCH Clearnet SA, enregistrée sous la dénomination sociale de Banque centrale de compensation). La CCP française propose des services de compensation des instruments financiers et assure la garantie de bonne fin des opérations sur quatre lignes d'activités :

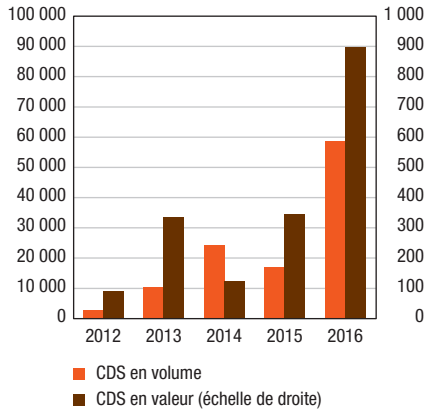
- produits listés au comptant : actions au comptant et obligations convertibles listées sur les marchés Euronext ;

- 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'État (italien, français, allemand, belge et espagnol). Cette ligne d'activité inclut €GC Plus, le service de compensation de pensions livrées *(repos)* dont le collatéral est géré de façon tripartite par Euroclear France ;

G1 LCH SA : dérivés de crédit (CDS)

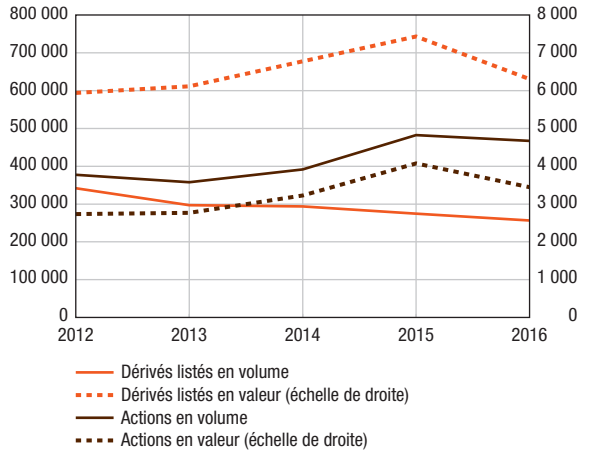
(volume en milliers d'opérations, valeur en milliards d'euros)



Source : Banque des règlements internationaux (BRI), *Statistics on payment, clearing and settlement systems in the CPMI countries (Red Book)* – 2017.

G2 LCH SA : opérations au comptant et dérivés sur actions

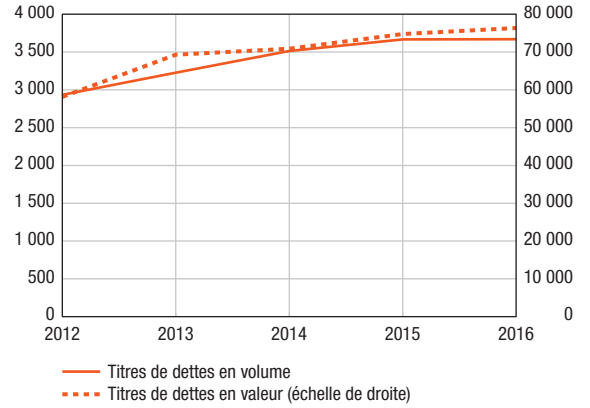
(volume en milliers d'opérations, valeur en milliards d'euros)



Source : Banque des règlements internationaux (BRI), *Statistics on payment, clearing and settlement systems in the CPMI countries (Red Book)* – 2017.

G3 LCH SA : opérations fermes et pensions sur titres d'État

(volume en milliers d'opérations, valeur en milliards d'euros)



Source : Banque des règlements internationaux (BRI), *Statistics on payment, clearing and settlement systems in the CPMI countries (Red Book)* – 2017.

• *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 [17].

Évolutions récentes et projets de développement

Sur le segment au comptant et dérivés, LCH SA a poursuivi et conforté en 2017 son offre de compensation auprès du marché réglementé Euronext.

Début août 2017, LCH SA et Euronext se sont mis d'accord sur la poursuite de la compensation des marchés de dérivés par la CCP française, pour une période de dix ans renouvelable. L'accord a été signé le 31 octobre 2017. Sur le segment actions au comptant, LCH SA reste également la principale CCP pour la compensation des marchés d'Euronext. Toutefois, Euronext a décidé fin 2016 d'ouvrir cette activité à la concurrence, en modifiant ses règles pour permettre, au choix des participants, de faire compenser les opérations au comptant soit par la CCP néérlandaise EuroCCP, soit par LCH SA (modèle dit *« preferred CCP »*).

Par ailleurs, ces évolutions ont été accompagnées de prises de participation dans les CCP partenaires. Euronext a ainsi acquis une participation de 20 % dans EuroCCP. Sa participation de 2,3 % dans LCH Group Ltd a été transformée en une participation de 11,1 % directement au capital de LCH SA. Le groupe LSE et Euronext sont également convenus de l'octroi d'un droit de

17 Les CDS sur indices compensés sont les suivants : iTraxx Europe Main, iTraxx Europe Crossover, iTraxx Europe HiVol ; CDS iTraxx Europe Senior Financials ; CDX North America Investment Grade et CDX North America High Yield. La CCP propose également depuis fin 2017 la compensation d'options sur les indices CDS iTraxx Europe Main et Crossover.

préemption dans le cas d'une vente de LCH SA au bénéfice d'Euronext, qui pourra être mis en œuvre sous certaines conditions, et notamment si le groupe LSE décide de vendre plus de 50 % du capital de LCH SA.

Les initiatives de LCH SA en lien avec Euronext ont été en outre importantes au cours de la période sous revue, avec le lancement en 2015 d'Atom X (nouvelle fonctionnalité, développée par Euronext, d'enregistrement de transactions effectuées en dehors du carnet d'ordres), de la compensation de divers nouveaux instruments (*single stock dividend futures, wood pellets* – contrats *futures* sur granules de bois à usage résidentiel), et en 2016 des instruments financiers dérivés sur les fertilisants azotés.

S'agissant de l'activité de compensation sur le segment *fixed income* (titres de dette et *repo*), la période a été marquée par une diversification de l'offre de compensation des dettes souveraines européennes libellées en euros. LCH SA a en effet lancé la compensation de la dette souveraine et assimilée allemande et de la dette belge (respectivement les 27 février et 29 novembre 2017), et devrait continuer à diversifier son offre de compensation des principales dettes souveraines européennes libellées en euros.

Concernant l'activité de compensation des CDS, 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 Senior Financials (indices et *single names*) en 2015 ;
- de CDS sur indices et *single names* américains libellés en dollars (CDX North American Investment Grade Index en mars 2016, puis CDX High Yield Index en décembre 2016) ;
- d'options sur indices CDS en 2017 (indices européen iTraxx Europe, Crossover iTraxx de 5 ans).

En outre, le segment CDSClear de LCH SA a progressé en termes de parts de marché, puisque la part de LCH SA dans la compensation de ces produits représente désormais environ 20 % des CDS libellés en euros et compensés en Europe.

Enfin, début 2017, LCH SA a lancé le projet *group member access* permettant à ses membres compensateurs d'accéder aux applications de compensation de LCH SA *via* une solution technique unique commune avec sa société sœur, LCH Ltd. Le projet de rationalisation des applications informatiques devrait se poursuivre dans le cadre d'un plan de transformation.

Évaluation

Les autorités nationales compétentes de la CCP sont la Banque de France, l'ACPR et l'AMF, qui exercent une supervision conjointe sous l'empire du règlement EMIR. LCH SA a par ailleurs le statut d'établissement de crédit et est supervisée à ce titre par l'ACPR ; elle relève également de la catégorie des établissements moins importants (*less significant institutions)* définies par le Mécanisme de supervision unique.

Les autorités nationales compétentes disposent de plusieurs modalités d'évaluation pour exercer leur rôle de supervision de la chambre de compensation. L'évaluation sur pièces conduite par les autorités est le mode le plus fréquent et le plus habituel : elle consiste à étudier les projets/changements proposés par la chambre de compensation sur la base de documents adressés aux autorités, de réunions régulières de suivi ou dédiées à des projets particuliers.

En parallèle de l'évaluation sur pièces, les autorités ont la possibilité de mener des inspections sur place. La dernière mission d'inspection de la Banque de France s'est déroulée chez LCH SA de novembre 2015 à mai 2016 et portait sur le dispositif de gestion du risque de liquidité. Cette mission avait pour objectif d'évaluer la robustesse du dispositif de gestion du risque de liquidité, élément

essentiel pour la CCP au regard de son agrément en tant que contrepartie centrale au titre du règlement EMIR, et indépendamment des facilités offertes par son statut d'établissement de crédit. Plus particulièrement, la mission d'inspection s'est concentrée sur les aspects relatifs à la gouvernance et au contrôle interne, la gestion opérationnelle de la liquidité, la gestion opérationnelle du défaut, le dispositif de *stress-testing*, et la gestion de la liquidité dans le cadre des relations avec la chambre de compensation italienne CC&G, avec laquelle LCH SA a un lien d'interopérabilité. Une lettre de suite à la mission d'inspection a été adressée début 2017 à la CCP sur un certain nombre de mesures correctrices à mettre en œuvre afin de renforcer le dispositif de gestion du risque de liquidité. Les actions correctrices sont intégrées au plan de supervision établi par les autorités françaises et font l'objet d'un suivi régulier.

Dans le contexte du règlement EMIR, les autorités nationales associent les autres autorités nationales européennes intéressées au bon fonctionnement de la chambre de compensation à la surveillance de l'infrastructure. La participation de ces autorités nationales est définie dans le règlement EMIR (article 18). Le collège EMIR est d'abord composé des autorités nationales compétentes qui surveillent la contrepartie centrale, mais aussi des autorités de surveillance des entités pour lesquelles les activités de la contrepartie centrale pourraient avoir un impact, à savoir les superviseurs des principaux membres compensateurs, des plateformes de négociation, des contreparties centrales interopérables et des dépositaires centraux de titres, les banques centrales d'émission des principales devises de l'UE traitées et l'AEMF, qui ne dispose pas de droit de vote.

Ce dispositif a pour objectif de permettre à la fois de promouvoir une approche homogène de la mise en œuvre des exigences d'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 dix-neuf autorités (dont l'AEMF), provenant de neuf pays différents 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 d'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.

Les autorités françaises ont organisé quatre collèges entre 2015 et 2017. Le collège se réunit une fois par an au minimum après instruction des sujets et peut être convoqué pour des réunions sur des sujets particuliers, ou en cas de crise.

2|2 Euroclear France et ESES France

Activité

Euroclear France, le dépositaire central de titres établi en France, offre les trois services de base définis par CSDR [18] : 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. Au-delà de ces trois services de base, Euroclear France offre plusieurs services dits « accessoires » tels que la

18 Cf. 1|4 pour plus de détails

gestion des opérations sur titres (versement de coupons et de dividendes, etc.), la gestion tripartite du collatéral, ou encore l'assignation d'un code ISIN aux nouveaux titres émis, etc.

ESES *(Euroclear Settlement of Euronext-zone Securities)* France constitue le système français de règlement de titres (ou système de règlement-livraison), qui a été connecté à TARGET2-*Securities* (T2S) le 12 septembre 2016. Aujourd'hui, la quasi-totalité des transactions et des opérations sur titres sont traitées sur T2S, auquel Euroclear France externalise le service de règlement de titres. Les établissements français qui ont un accès direct au système de règlement de titres n'ont ainsi de relation contractuelle qu'avec Euroclear France, qu'ils soient techniquement *directly connected parties* ou *indirectly connected parties* en T2S, et n'ont aucun lien contractuel avec T2S.

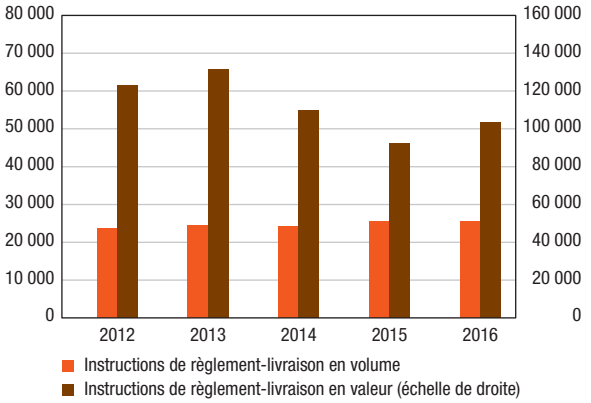
Depuis 2010, les CSD belge et néerlandais sous-traitent à Euroclear France la gestion opérationnelle de leur activité de règlement-livraison.

ESES France traite environ 90 % des valeurs réglées par les trois CSD ESES. D'après les données de l'ECSDA[19] *(European Central Securities Depositories Association)*, environ 12 % des titres européens sont en dépôt auprès d'Euroclear France, et un peu moins de 10 % des transactions sur titres réglées-livrées en Europe le sont par Euroclear France. La valeur des titres en dépôt a progressé d'environ 3 % en 2016, pour atteindre 6 300 milliards d'euros ; la valeur des instructions réglées-livrées a quant à elle connu une progression plus importante de l'ordre de 12 %, pour atteindre 103 000 milliards d'euros (cf. graphique 4).

19 *https://ecsda.eu/*

G4 Instructions de règlement-livraison traitées par ESES France

(volume en milliers d'opérations, valeur en milliards d'euros)



Source : Banque des règlements internationaux (BRI), *Statistics on payment, clearing and settlement systems in the CPMI countries (Red Book)* – 2017.

Évolutions récentes et projets de développement

Euroclear France a migré avec succès le 12 septembre 2016 vers la plateforme de règlement-livraison paneuropéenne T2S, lors de la troisième vague de migration. Cette réussite a marqué l'aboutissement d'un important processus d'adaptation opérationnel et juridique à cet environnement harmonisé. La préparation de cette migration, qui reposait en partie sur des tests d'une complexité grandissante impliquant un nombre croissant de parties prenantes, a été suivie de façon étroite par la Banque de France et l'AMF en 2015 et 2016.

La grande majorité des CSD européens (à l'exception des CSD internationaux Euroclear Bank et Clearstream Bank Frankfurt) a migré à T2S, notamment le CSD italien, Monte Titoli, qui a rejoint T2S lors de la première vague de migration en juin 2015. Le CSD allemand Clearstream Banking Frankfurt a quant à lui rejoint la plateforme en février 2017 lors de la quatrième vague de migration. Euroclear France, qui avait établi deux liens relayés vers ces CSD (avec Euroclear Bank comme CSD intermédiaire), les a transformés en liens directs « internes T2S » et a donc pu offrir à ses participants du règlement DvP (*delivery versus payment* – livraison contre paiement) en temps réel pour les titres émis ou détenus en Allemagne et en Italie, de façon analogue aux transactions domestiques sur les titres émis en France et pour un coût identique.

Évaluation

La surveillance des systèmes de règlement-livraison et des CSD ESES (Euroclear France, Euroclear Nederland et Euroclear Belgium) fait l'objet d'un dispositif de coopération entre les autorités françaises, belges et néerlandaises, responsables de la surveillance et de la régulation des dépositaires centraux et des systèmes de règlement de titres du groupe Euroclear. Un protocole d'accord conclu en juillet 2011 définit les modalités de leur coopération et de leurs échanges d'informations en matière de réglementation et de contrôle des opérations de règlement-livraison. La Banque nationale de Belgique (BNB) a été désignée pour présider et organiser les réunions entre autorités ainsi que certains échanges d'information avec les CSD ESES ; la Banque de France y participe en tant que surveillant d'ESES France. Chaque superviseur/surveillant d'ESES reste néanmoins responsable dans l'exercice de ses fonctions et prérogatives vis-à-vis du SSS/CSD national, *a fortiori* au vu des prérogatives accordées aux autorités compétentes par le règlement européen CSDR. Le dispositif actuel a été maintenu (avec des adaptations pour tenir compte de ces prérogatives réglementaires), ce qui permet une coordination importante de l'étude des sujets CSDR par les autorités françaises, belges et néerlandaises, en cohérence avec le fonctionnement et les caractéristiques très similaires des trois CSD ESES.

Des évaluations formalisées du système de règlement-livraison de titres au regard des normes internationales (PFMI) ont été réalisées régulièrement, généralement tous les trois ans. Le processus d'évaluation établi selon ces principes est désormais remplacé par les dispositions du règlement CSDR depuis l'entrée en vigueur de ce dernier. La dernière évaluation des CSD ESES, dont Euroclear France, et de leur système de règlement-livraison, a été publiée en septembre 2015 sur le site de la Banque de France. Cette évaluation est le résultat du travail conjoint de six autorités, composées des banques centrales et des autorités de marché de chacun des trois pays d'établissement des CSD ESES. L'évaluation a conclu à la pleine conformité des CSD ESES à l'ensemble des principes applicables, à l'exception de trois principes considérés comme globalement respectés : le principe 19 relatif aux dispositifs à plusieurs niveaux de participation, le principe 20 relatif aux liens entre infrastructures de marché, et le principe 23 relatif à la communication des règles, procédures clés et données de marché.

Depuis la mise en œuvre de CSDR, la Banque de France est non seulement l'autorité de surveillance du système de règlement-livraison ESES France en vertu des missions qui lui sont dévolues dans le *Code monétaire et financier*, mais aussi autorité compétente d'Euroclear France. L'AMF est elle aussi autorité compétente d'Euroclear France sous CSDR, et était déjà l'autorité de supervision d'Euroclear France dans le cadre français.

Euroclear France est en cours d'agrément au regard de CSDR (cf. section 1.4). Pour cela, il a déposé un dossier en septembre 2017, qui est en cours d'étude par les autorités compétentes.

La mise en œuvre de CSDR implique des modifications chez les CSD européens, afin de se mettre en conformité avec les dispositions harmonisées introduites par ce règlement. La plupart de ces changements avaient déjà été introduits, ou étaient en cours de mise en œuvre à la suite des évaluations de surveillance à l'aune des PFMI. À titre d'exemple, l'établissement d'un plan de rétablissement adéquat par les CSD fait maintenant partie des exigences réglementaires applicables, et conduit à affiner annuellement le plan de rétablissement des CSD ESES dont la première version date de 2014.

2|3 CORE(FR)

Activité

CORE(FR), le système de paiement de détail français, est exploité par la société STET (Systèmes technologiques d'échanges et de traitement).

Il permet à ses participants, qui sont des banques françaises, de présenter sous la forme de remises groupées les opérations de paiement de détail nationales. Ces opérations font ensuite l'objet d'une compensation quotidienne permettant de calculer le solde net de chaque participant. Le règlement des positions nettes multilatérales intervient quotidiennement dans TARGET2-Banque de France à 15 heures.

En 2017, 12,5 milliards d'opérations ont été compensées dans CORE(FR), représentant en valeur 4 800 milliards d'euros. De 2014 jusqu'à fin 2016, les opérations compensées dans CORE(FR) ont progressé en volume de 4,4 % et en valeur de 3,1 %. Le volume des flux dans CORE(FR) a diminué à la fin de l'année 2016, en raison de la migration de la compensation des prélèvements bancaires au format européen SEPA [20] (*SEPA Direct Debit* – SDD) de CORE(FR) vers le nouveau système SEPA.EU, créé en novembre 2016, et également exploité par la société STET (cf. section 2.4). Sur l'année 2017, entre 949 et 1 144 millions d'opérations ont été réglées mensuellement, représentant des valeurs oscillant entre 370 et 452 milliards d'euros. L'évolution de l'activité dans CORE(FR), en volume et en valeur, est schématisée dans les graphiques 5a et 5b.

CORE(FR) bénéficie 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 (800,5 millions d'euros à fin 2016, ramené à 650,5 millions d'euros en novembre 2017), ainsi qu'en complément, 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 BNB.

Évolutions récentes et projets de développement

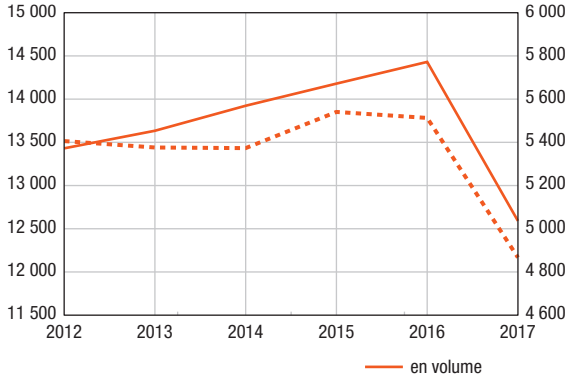
Le 21 novembre 2016, la société STET a assuré le lancement opérationnel de SEPA.EU, système paneuropéen de compensation et de règlement des paiements SEPA. Les prélèvements bancaires SDD qui étaient auparavant traités dans CORE(FR)

20 *Single Euro Payments Area*

G5 Activité dans CORE(FR)

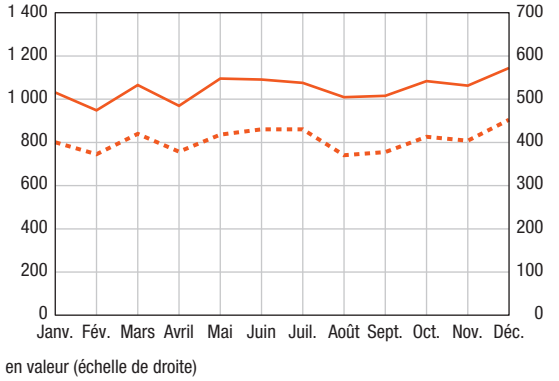
a) depuis 2012

(volume en millions d'opérations, valeur en milliards d'euros)



b) en 2017

(volume en millions d'opérations, valeur en milliards d'euros)



Sources : STET, Banque de France.

sont désormais traités et compensés dans SEPA.EU (cf. section 2.4). Ce changement majeur a donné lieu à une pré-évaluation de la Banque de France afin de s'assurer du respect par le futur système des principes qui lui sont applicables. Le bon déroulement de la migration de ces instruments de CORE(FR) vers SEPA.EU a été assuré grâce notamment à une consultation régulière du comité clients de CORE(FR) – instance de gouvernance du système – et de comités techniques, ainsi qu'à une mise en cohérence des règles de fonctionnement du système avec les règles transposées de l'*European Payments Council* (EPC) pour le virement et le prélèvement, et enfin à un dimensionnement adéquat des moyens techniques.

La Banque de France a suivi ces différentes activités et évalué la conformité de leurs conditions de mise en œuvre avec le cadre de surveillance afin d'assurer le maintien de la sécurité et de l'efficacité de CORE(FR) pendant et après cette migration.

Évaluation

Sur la base des critères de classification du règlement BCE n° 795/2014 relatif aux exigences de surveillance applicables aux systèmes de paiement d'importance systémique (SPIS), CORE(FR) a été désigné en août 2014 par le Conseil des gouverneurs de la BCE comme un SPIS, aux côtés des systèmes paneuropéens TARGET2, EURO1 et STEP2-T. En effet, CORE(FR) remplit deux des quatre critères fixés par le règlement : la valeur des paiements quotidiennement réglés dans le système (supérieure à dix milliards d'euros) et la part de marché au regard du volume total des paiements libellés en euros [21].

La Banque de France a été désignée le 13 août 2014 par le Conseil des gouverneurs de la BCE comme autorité compétente pour la surveillance de CORE(FR). La BCE étant en charge de la surveillance des trois autres systèmes paneuropéens précités, la Banque de France est donc à ce jour la seule banque centrale nationale de l'Eurosystème en charge de la surveillance d'un SPIS.

Le rapport d'évaluation de CORE(FR) au regard des exigences du règlement BCE n° 795/2014 a été finalisé par la Banque de France en 2016, en lien avec l'évaluation par l'Eurosystème des trois autres systèmes de paiement d'importance systémique. Le système a été jugé globalement conforme au règlement. Au moment de la finalisation de l'évaluation, au 31 janvier 2016, plusieurs actions devaient être entreprises par l'opérateur pour assurer la pleine conformité du système à toutes les dispositions du règlement.

L'opérateur STET a mis en œuvre depuis l'évaluation la plupart des actions demandées et les actions résiduelles font l'objet d'un suivi et d'une communication rapprochés par la Banque de France et d'un reporting régulier auprès de l'Eurosystème.

Par ailleurs, la Banque de France a transmis à l'opérateur des recommandations, qui ont été pour la plupart également mises en œuvre, visant, au-delà des exigences du règlement BCE, à améliorer encore le cadre de gestion des risques du système.

2|4 SEPA.EU

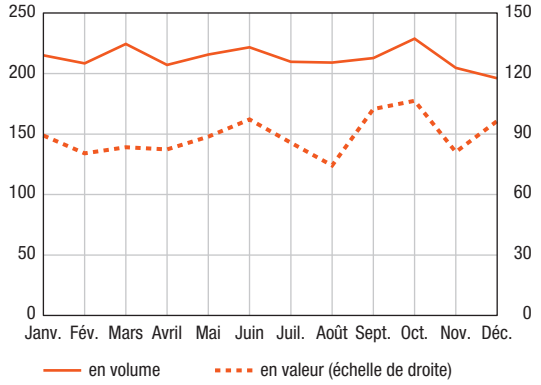
Activité

SEPA.EU est le système de paiement de détail à vocation paneuropéenne opéré par la société STET, également opérateur de CORE(FR). SEPA.EU, dont l'activité a démarré le 21 novembre 2016, a pour objet le règlement des moyens de paiement SEPA, à savoir les virements (SEPA *Credit Transfers* – SCT) et les prélèvements bancaires (SEPA *Direct Debits* – SDD). Dans une première phase, avant le déploiement de son service à l'échelle européenne, SEPA.EU sert la communauté de banques françaises également participantes à CORE(FR). Depuis son lancement, le système traite et compense les prélèvements bancaires, auparavant traités dans CORE(FR).

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

G6 Activité dans SEPA.EU en 2017

(volume en millions d'opérations, valeur en milliards d'euros)



Sources : STET, Banque de France.

Du 21 novembre au 30 décembre 2016, 235,65 millions de transactions (prélèvements SDD) ont été réglées dans SEPA.EU, pour un montant de 120,48 milliards d'euros. Sur l'année 2017, le volume des transactions réglées est stable (entre 196 et 229 millions de transactions par mois) et les valeurs mensuelles traitées oscillent entre 74 et 106 milliards d'euros (cf. graphique 6).

Évolutions récentes et projets de développement

Les projets en cours sont les suivants :

- la bascule des virements SCT de CORE(FR) vers SEPA.EU : STET procédera à la migration du système CORE(FR) vers SEPA.EU des virements bancaires SCT en mars 2019. Contrairement au dispositif existant sur CORE(FR), qui repose sur un cycle unique de 24 heures, la notion de cycle disparaîtra dans SEPA.EU, au profit d'un règlement en continu, assorti d'un préfinancement ;

- le lancement d'un service optionnel de règlement des paiements instantanés : CSM [22] *Instant Payment* est un service de règlement des virements instantanés répondant au *scheme* développé par l'EPC, SCT Inst [23], qui sera intégré à SEPA.EU. Ce projet est commun aux communautés bancaires française et belge, même si les calendriers de mise en œuvre du service sont distincts. Le lancement officiel du service sur le marché est planifié pour novembre 2018. Cette initiative fera l'objet d'une pré-évaluation menée par la Banque de France, afin d'analyser si les changements générés dans SEPA.EU par le CSM *Instant Payment* sont susceptibles d'entraîner des modifications dans la conformité aux neuf principes pour les infrastructures des marchés financiers auquel est soumis SEPA.EU (cf. *infra*). En outre, la gestion du risque opérationnel fera l'objet d'une surveillance partagée entre la Banque de France et la BNB, dans le cadre du *memorandum of understanding* établi entre les deux autorités.

Évaluation

Si CORE(FR) et SEPA.EU sont deux systèmes distincts sur le plan juridique, ils présentent néanmoins des caractéristiques communes. Depuis son lancement, SEPA.EU opère en effet sur la même plateforme technique que CORE(FR) et est régi par une gouvernance identique. Néanmoins, dans la mesure où SEPA.EU a vocation à devenir un système autonome de CORE(FR) à moyen terme, la Banque de France, dans sa mission de surveillance, considère SEPA.EU comme un système à part entière, qui a été notifié en tant que tel au titre de la directive finalité par l'AEMF en novembre 2016 et est inclus dans la liste des systèmes de paiement et de règlement de titres désignés dans cette directive et opérant en France.

La Banque de France est l'autorité compétente en charge de la surveillance, en application de l'article L141-4 du *Code monétaire et financier*. Dans la mesure où SEPA.EU règle, sur une base annuelle, des volumes de paiements 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 [24]. L'évaluation de cette catégorie de système de paiement est conduite au regard du respect de neuf

22 *Clearing and Settlement Mechanism*

23 L'EPC SCT Inst est un *scheme* paneuropéen fondé sur le virement SEPA, établi par le Conseil des paiements européens, dont l'objectif est d'aboutir au traitement d'une transaction en temps réel, 365 jours par an, 7 jours sur 7 et 24 heures sur 24.

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

principes CPMI-IOSCO pour les infrastructures des marchés financiers [25] (PFMI).

Le rapport d'évaluation de SEPA.EU à l'aune des exigences des PFMI applicables aux ORPS a été finalisé par la Banque de France en juillet 2017. Le système a été jugé globalement conforme aux neuf principes qui lui sont applicables. À la suite de cette évaluation, l'opérateur STET a transmis, en septembre 2017, à la Banque de France un plan d'actions, afin de proposer des mesures correctrices répondant aux recommandations du surveillant. La mise en œuvre des recommandations résiduelles fait l'objet d'un suivi rapproché par la Banque de France et d'un reporting auprès de l'Eurosystème.

2|5 La surveillance coopérative

Contreparties centrales européennes

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 Compenzacione e Garanzia), avec qui la CCP française a un lien d'interopérabilité, de la CCP allemande Eurex Clearing AG et de la CCP néerlandaise EuroCCP, en tant que surveillant du dépositaire central de titres (Euroclear France) auquel ces CCP sont liées. La Banque de France est également suppléante de la BCE en tant que banque centrale d'émission au collège EMIR de la CCP britannique LCH Ltd.

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, à savoir la Banque de France, Deutsche Bundesbank et Banca d'Italia. En 2016, 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 : la Bulgarie, la Croatie, le Danemark, la Pologne et la Roumanie.

A l'instar du système français CORE(FR), TARGET2 a été identifié comme système de paiement d'importance systémique, par une décision du Conseil des gouverneurs d'août 2014, et, par conséquent, est soumis aux exigences du règlement de la BCE n° 795/2014 du 3 juillet 2014, révisé par le règlement 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 participant au système.

Le système TARGET2 a fait l'objet d'une évaluation conduite en 2015, sous l'égide de la Banque centrale européenne et de façon conjointe avec les banques centrales de la zone euro volontaires pour mener l'exercice d'évaluation.

Au moment de la finalisation de l'évaluation, au 31 janvier 2016, plusieurs actions devaient être entreprises par l'opérateur pour assurer la pleine conformité du système à toutes les dispositions du règlement. L'opérateur TARGET2 a mis en œuvre depuis l'évaluation la plupart des actions demandées et les actions résiduelles font l'objet d'un suivi et d'une communication rapprochés par la BCE.

TARGET2-*Securities*

Si TARGET2-*Securities* (T2S) ne correspond pas à la définition de « système » de règlement de titres au sens de la directive sur la finalité des règlements et n'est donc pas surveillé à ce titre, son caractère systémique en tant que plateforme paneuropéenne de règlement-livraison 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

25 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).

et des conclusions par l'ensemble des banques centrales nationales (BCN).

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 co-présidence de cette instance coopérative du groupe de surveillance par la BCE et par l'AEMF. Les 24 CSD ayant migré lors des cinq vagues initiales de migration à T2S sont établis dans 21 États membres de l'UE et de l'Espace économique européen, le groupe de surveillance réunit donc 21 BCN et 21 autorités nationales de marché, en plus de l'AEMF et de la BCE.

Une évaluation préliminaire de T2S au regard des normes ESCB-CESR[26] a été achevée début 2014, puis publiée par la BCE et l'AEMF. L'évaluation de certaines normes restait à finaliser, en particulier celle sur la finalité du règlement, dans l'attente de règles communes, finalisées et juridiquement opposables aux tiers. Depuis, la surveillance de la partie « espèces » de T2S fait partie de l'évaluation globale de TARGET2[27], car les comptes espèces sont juridiquement dans les systèmes nationaux composant TARGET2 (par exemple TARGET2-Banque de France), et s'effectue au regard des PFMI.

T2S fera l'objet d'une nouvelle évaluation de surveillance exhaustive à partir de début 2018, cette fois-ci à l'aune des PFMI. L'opérateur de T2S devra dans un premier temps fournir une autoévaluation en répondant à un questionnaire ; l'évaluation finale sera conduite sur la base de cette autoévaluation, analysée de façon critique en la confrontant notamment à l'ensemble de la documentation T2S (éléments contractuels, manuels opérationnels, etc.). Un certain nombre de sujets fera l'objet d'une évaluation pour la première fois sur le fond, notamment la finalité des règlements en T2S grâce à la signature d'un accord de principe par l'ensemble des CSD et banques centrales participant à T2S, une transposition concrète de ces principes par des procédures communes et la livraison de nouvelles fonctionnalités en T2S.

EURO1 et STEP2-T

Sous l'égide de la BCE qui assume le rôle de surveillant principal, la Banque de France participe à la surveillance coopérative des systèmes de paiement exploités par la société EBA Clearing, qui sont des systèmes paneuropéens : EURO1 (système de paiement de montant élevé) et STEP2 (système de paiement de détail pour le traitement des virements SCT et des prélèvements SDD).

La Banque de France a contribué à différents travaux d'évaluation conduits par la BCE concernant notamment la conformité des dispositifs des deux systèmes à la réglementation sur les systèmes de paiement d'importance systémique (cf. section 1|3), ainsi que le suivi des plans d'action, et la mise en œuvre du système RT1 qui est la solution paneuropéenne *Instant Payment* d'EBA Clearing, opérationnelle depuis le 21 novembre 2017.

SWIFT

Dans le cadre de la surveillance coopérative de SWIFT menée par la BNB, à laquelle la Banque de France participe, les travaux de surveillance de la période sous revue ont notamment porté sur le *customer security programme*, un programme à destination de tous les clients de SWIFT visant à améliorer la cyber-sécurité de leur environnement domestique, la prévention et la détection des attaques et les processus de réaction en cas d'incident :

- en participant à la consultation publique menée par SWIFT ;
- en donnant un accord à SWIFT pour poursuivre les différents pans de son programme après étude de chaque principe et document fondateur ;

26 Les normes ESCB-CESR étaient des normes non contraignantes adoptées par les régulateurs européens pour la surveillance notamment des CSD et des SSS *(securities settlement systems)*. Elles ont été remplacées en 2012 par les PFMI.

27 Rapport de l'évaluation de TARGET2 par rapport aux PFMI : *http://www.ecb.europa.eu/pub/pdf/other/t2disclosurereport201606.en.pdf?8341c2a74d87b322292738afa9c331a3*

• en intervenant auprès de la communauté des utilisateurs de SWIFT lors de la série de présentations du programme.

CLS

Le système CLS permet le règlement en mode PvP (*payment versus payment* – paiement contre paiement) des instructions de paiements 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[28] 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 démarré son activité de règlement en septembre 2002. Fin 2015, il comptait 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 (le *Protocol for the Cooperative Oversight Arrangement of CLS*) entre les banques centrales, celles du groupe des dix (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.

28 La structure juridique de CLS se compose de CLS Group Holding AG, une société *holding* sous droit suisse, représentant les actionnaires (les banques participantes), qui détient elle-même CLS UK Intermediate Holding, une société sous droit anglais qui fournit différents services à ses filiales, CLS Bank International et CLS Services Ltd. CLS Bank International est basée à New-York, tient les comptes des participants, alors que CLS Services Ldt, basée à Londres, fournit les services opérationnels à CLS Bank International.

La surveillance des moyens de paiement scripturaux entre 2015 et 2017

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

1.1 La mise en œuvre de la deuxième directive européenne sur les services de paiement

La convergence des réglementations applicables au marché des paiements est une composante essentielle à l'intégration de ce marché en Europe, et vient compléter les initiatives politiques majeures telles que l'introduction de l'euro fiduciaire ou la mise en place des moyens de paiement SEPA *(Single Euro Payments Area)*. La première directive européenne sur les services de paiement et les deux directives européennes sur la monnaie électronique, adoptées dans les années 2000, visaient à apporter un cadre harmonisé en matière de régulation des services de paiement en Europe, tout en renforçant à la fois la protection du consommateur et la concurrence sur ce marché.

La deuxième directive européenne sur les services de paiement (DSP2), adoptée le 25 novembre 2015, et entrée en vigueur le 13 janvier 2018, s'inscrit dans le prolongement de ces textes, en étendant le champ des services de paiement régulés à de nouveaux services et acteurs, tout en renforçant les exigences sécuritaires applicables aux acteurs du marché des paiements. Après avoir été associée aux négociations qui ont mené à l'adoption de la directive, la Banque de France a été largement impliquée dans les travaux de rédaction de l'ordonnance de transposition parue au *Journal officiel* le 10 août 2017.

La DSP2 crée un statut de prestataire de services de paiement (PSP) pour les acteurs tiers qui accèdent aux comptes tenus par des PSP dits « gestionnaires de comptes » (principalement les banques) pour initier des paiements ou pour agréger les informations de comptes :

- l'initiateur de paiement est un intermédiaire qui a la capacité d'initier des paiements, le plus souvent des virements, depuis le compte bancaire en ligne du client, et propose notamment ces offres de paiement aux commerçants en ligne comme une alternative possible au paiement par carte ou par portefeuille électronique ;

- l'agrégateur d'information propose un service de consolidation des informations des différents comptes de paiement qu'un client peut détenir auprès d'autres prestataires de services de paiement.

Ces activités, exercées jusqu'alors en dehors de tout cadre réglementaire, présentent un risque élevé en matière de fraude car elles nécessitent la communication par les utilisateurs à un tiers des identifiants et codes d'accès des comptes bancaires en ligne. Dans ce nouveau cadre, le texte prévoit que les identifiants bancaires peuvent être partagés

avec les PSP tiers, tout en assurant leur protection, notamment par le chiffrement des données. Il est également prévu que les PSP tiers et les PSP gestionnaires de comptes, ainsi que les utilisateurs, communiquent de façon sécurisée en utilisant une interface dont les principes sont spécifiés par un texte réglementaire dit de niveau 2 associé à la directive.

La directive défend également un objectif d'amélioration de la sécurité des paiements, articulé autour des deux axes suivants :

• l'authentification forte du titulaire du compte est requise pour l'accès aux comptes et pour toute action en ligne qui présente des risques importants (par exemple, création d'un nouveau bénéficiaire pour les virements sur un espace de banque en ligne) ;

• l'authentification forte du payeur (cf. encadré 3) est requise pour l'initiation de paiements par voie électronique.

Cette obligation de recours à l'authentification forte peut toutefois faire l'objet d'exemptions définies réglementairement dans le cas où les transactions sont considérées comme peu risquées (par exemple, paiement de faible montant ou virement entre plusieurs comptes d'une même personne).

L'Autorité bancaire européenne (ABE) a ainsi reçu pour mandat d'élaborer, en étroite collaboration avec la Banque centrale européenne (BCE), une norme technique de réglementation qui précise : i) les requis et les exemptions de l'authentification forte des clients pour la sécurisation des transactions et des accès aux comptes ; ii) les requis en matière de protection des identifiants de connexion ; iii) les modalités techniques et opérationnelles permettant aux banques, aux PSP tiers et à leurs clients de communiquer de façon sécurisée. Pour permettre aux acteurs d'adapter leurs systèmes informatiques, il est prévu que les dispositions de la directive précisées par cette norme technique seront applicables dix-huit mois après l'adoption de cette norme.

En complément de sa contribution à l'élaboration de cette norme technique de réglementation, la Banque de France a également participé à l'élaboration de deux autres textes précisant des dispositions de la directive et ayant trait à sa mission de surveillance des moyens de paiement :

• une orientation de l'ABE relative aux notifications des incidents majeurs, qui a été publiée le 27 juillet 2017 ;

• une orientation de l'ABE sur la gestion des risques opérationnels et de sécurité, qui a été publiée le 12 décembre 2017.

Ces deux orientations sont rentrées en application en même temps que la DSP2, c'est-à-dire le 13 janvier 2018.

1|2 Le paiement instantané : le *scheme* SCT Inst de l'*European Payments Council*

Dans un contexte où, en lien avec le développement du commerce électronique, la rapidité d'exécution des opérations constitue l'un des enjeux majeurs de la modernisation des paiements, le sujet des paiements dits « instantanés » est devenu central au cours des dernières années. Pour cette raison, l'*Euro Retail Payments Board* (ERPB) a lancé en décembre 2014 des travaux européens en la matière, qui l'ont conduit, d'une part, à définir les paiements instantanés comme des solutions de paiement électronique disponibles 24 heures sur 24, permettant un règlement interbancaire et un crédit en compte du bénéficiaire immédiats, et, d'autre part, à charger les acteurs de l'industrie européenne de développer une solution paneuropéenne dans les meilleurs délais.

Ces travaux ont abouti, en novembre 2016, à la présentation par l'*European Payments Council* (EPC) d'un projet paneuropéen de paiements instantanés conformes à la définition de l'ERPB.

Encadré 3

L'authentification forte du payeur

La question de la sécurisation des paiements sur internet a été soulevée dès 2008, dans l'enceinte de l'Observatoire de la sécurité des cartes de paiement (OSCP) sous l'impulsion de la Banque de France. Les recommandations émises par l'Observatoire dans son rapport annuel 2009 définissaient le concept d'authentification forte du payeur, et invitaient les acteurs du marché français des cartes de paiement à développer et mettre en œuvre des solutions d'authentification répondant à cette définition.

L'exemple français a inspiré les travaux conduits au niveau européen, tout d'abord dans le cadre du forum européen *SecuRe Pay*, puis de la Commission européenne en préparation de la deuxième directive sur les services de paiement (DSP2). La nouvelle directive définit ainsi l'authentification forte comme un ensemble de procédures fondées sur l'utilisation d'au moins deux éléments parmi les trois suivants :

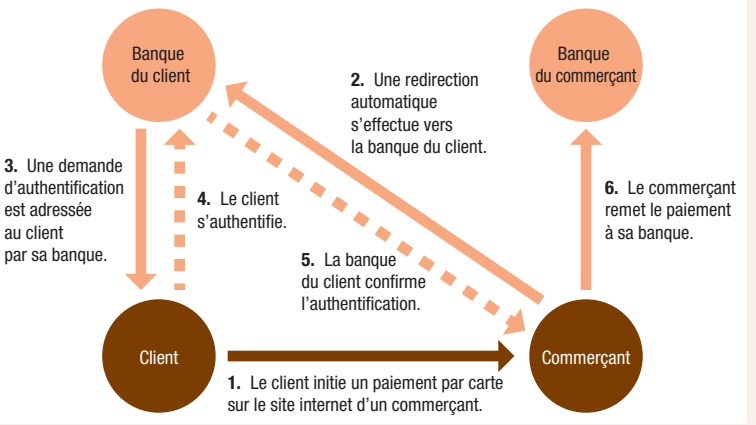
- élément connu du seul payeur : il s'agit d'un élément que le payeur est le seul à connaitre, comme un mot de passe, un code d'identification personnel (code PIN), etc. ;

- élément en la possession du seul payeur : il s'agit d'un élément dont le payeur est le seul détenteur, comme un *token*, un téléphone mobile, une carte à microprocesseur (carte à puce), etc. ;

- élément lié à la personne elle-même : il s'agit d'une caractéristique biométrique du payeur telle que l'empreinte digitale ou la voix par exemple.

Les éléments retenus doivent être mutuellement indépendants, au sens où la compromission de l'un ne doit pas mettre en danger la sécurité des autres. En outre, l'un des éléments choisis au moins doit être non rejouable et non reproductible (excepté pour la biométrie). Enfin, la procédure d'authentification forte doit assurer la protection de la confidentialité des données d'authentification.

Le dispositif d'authentification forte le plus répandu actuellement pour les paiements sur internet repose sur un code à usage unique tel un OTP *(one time password)* communiqué au payeur selon divers canaux possibles (envoi d'un SMS sur son téléphone portable, génération sur le site de banque en ligne du payeur, par un lecteur de carte physique, une *display card*, un *token*, etc.) [1]. Lors du paiement, la page de paiement en ligne met en relation le payeur avec la banque qui a émis la carte pour qu'elle puisse l'authentifier, en s'appuyant sur le protocole *3D-Secure* dont le fonctionnement est synthétisé dans le schéma ci-contre.



1 Le rapport annuel 2015 de l'Observatoire de la sécurité des cartes de paiement présente un état des lieux des techniques d'authentification renforcée les plus couramment utilisées en France : *https://www.banque-france.fr/sites/default/files/medias/documents/oscp-rapport-annuel-2015.pdf*

Encadré 4

L'accompagnement du développement des fintechs dans le domaine des paiements en France

Les fintechs (contraction des termes « finance » et « technologie ») sont des entreprises innovantes qui développent des services à valeur ajoutée en appliquant à l'univers de la banque, de la finance et de l'assurance les technologies numériques les plus avancées (technologies mobiles et de télécommunication, biométrie, intelligence artificielle, *big data*, *blockchain*, etc.).

Dans le domaine des paiements, les fintechs représentent un fort potentiel de croissance. Des mesures spécifiques ont ainsi été prises par les autorités françaises en vue de faciliter leur développement :

• des statuts réglementaires adaptés au lancement des fintechs : la loi n° 2016-1321 pour une République numérique adoptée et promulguée le 7 octobre 2016, a modifié le *Code monétaire et financier* en introduisant une disposition qui devrait faciliter le développement des fintechs, en anticipation de la transposition de la deuxième directive sur les services de paiement (DSP2). Désormais les entreprises qui fournissent des services de paiement utilisables uniquement au sein d'un réseau limité d'accepteurs ou pour l'achat d'un éventail limité de biens ou de services, et dont le volume d'activité sur douze mois est inférieur à un million d'euros, n'ont plus aucune démarche à faire auprès de l'Autorité de contrôle prudentiel et de résolution (ACPR). La loi française prévoit également depuis plusieurs années des agréments d'établissements de paiement (EP) et d'établissements de monnaie électronique (EME) à statut prudentiel allégé, avec des exigences moindres en termes de capital minimum et de fonds propres. Les établissements agréés sous ces statuts peuvent en bénéficier dès lors que leur volume d'activité est faible (trois millions d'euros de paiements gérés mensuellement pour les EP, une moyenne mensuelle de cinq millions d'euros de monnaie électronique en circulation pour les EME). Toutefois, ces statuts allégés ne permettent pas la délivrance d'un passeport européen ;

• concernant les nouveaux services d'agrégation d'information sur les comptes et d'initiation des paiements, la Banque de France, tout comme l'ACPR, a rencontré en amont de l'entrée en vigueur de la DSP2 les fintechs candidates aux nouveaux statuts apportés par la directive, afin notamment de les accompagner dans l'élaboration de leurs dossiers d'agrément. Pour la Banque de France, l'objectif principal était d'apporter des éclairages sur les dispositions relatives à la sécurité de ces deux nouveaux services ;

• les actions de surveillance exercées par la Banque de France couvrent l'ensemble du cycle de vie des fintechs : de l'agrément des EP et EME pour évaluer la sécurité des services de paiements proposés à la collecte annuelle de données statistiques et d'informations réglementaires. Ces actions sont guidées par deux principes complémentaires : i) un socle minimal d'exigences en matière de sécurité, portant notamment sur la protection des données sensibles de paiement et les méthodes d'authentification ; ii) une approche proportionnée aux risques pour l'application des exigences de surveillance (en matière de gouvernance, maîtrise des risques, continuité, etc.).

Cette solution doit permettre de réaliser, 24 heures sur 24 et 7 jours sur 7, des opérations de paiement en euros en moins de dix secondes, sous la forme de virements SEPA instantanés (appelés SCT Inst). Elle peut être mise en œuvre par les prestataires de services de paiement adhérents de l'EPC depuis novembre 2017, date d'entrée en vigueur du *scheme* SCT Inst retenue par l'EPC ; l'adhésion à ce *scheme* par les banques étant toutefois facultative, ces dernières sont libres de proposer ou non des offres de services basées sur le virement instantané à leurs clients.

Afin de préparer au mieux au niveau français la mise en place de cette solution de paiement paneuropéenne, le Comité national des paiements scripturaux (CNPS) a identifié en 2016 les conditions de développement des offres liées au virement instantané, en portant une attention particulière aux avantages et risques liés à son utilisation et en définissant ses différents cas d'usage envisageables.

Par ailleurs, pour favoriser une adoption rapide et sûre de ce nouveau mode de paiement, la BCE et l'ensemble des banques centrales de l'Eurosystème conduisent depuis juin 2017 un exercice commun d'évaluation du *scheme* SCT Inst au regard du cadre de surveillance applicable. Les enseignements de cet exercice devraient être communiqués au printemps 2018 par la BCE.

1|3 La mise en place du Comité national des paiements scripturaux

Succédant au Comité national SEPA, le CNPS a été créé en avril 2016. Présidé par la Banque de France, avec une vice-présidence assurée par l'Association française des trésoriers d'entreprise (AFTE) et la Fédération bancaire française (FBF), ce Comité a vocation à offrir une structure de dialogue pour l'ensemble des acteurs français des moyens de paiement (représentants de la demande, de l'offre et des autorités publiques) qui contribue à assurer à la fois la bonne mise en œuvre de la stratégie nationale des paiements scripturaux, lancée en octobre 2015 par le ministère de l'Économie [1] et des Finances, et l'influence de la communauté française sur l'évolution des systèmes de paiement européens.

À cette fin, les travaux du Comité ont été organisés autour de trois priorités :

• la diversification de l'offre de paiement du secteur public. Le Comité a offert un cadre de concertation autour des initiatives des acteurs de la sphère publique et sociale, dont l'objectif est de proposer aux cotisants des moyens de paiement mieux adaptés à leurs besoins, ainsi qu'à ceux de la sphère publique ;

• l'utilisation par les entreprises des nouveaux instruments de la gamme SEPA et en particulier le virement dit « instantané », qui fait l'objet d'un projet paneuropéen piloté par l'ERPB. Le Comité a ainsi lancé des travaux fonctionnels et techniques pour assurer la bonne mise en œuvre du virement instantané en France. Il s'est également attaché à valoriser les fonctionnalités de référencement comptable des ordres de paiement électroniques tels que le virement SEPA, identifié comme un prérequis important à l'utilisation de ce moyen de paiement pour de nombreuses entreprises. La diffusion de ces moyens de paiement doit permettre d'accompagner la décroissance de l'utilisation du chèque, en s'inscrivant comme des alternatives, en particulier pour les paiements entre entreprises ;

• l'utilisation par le grand public d'instruments électroniques rapides, sûrs et accessibles, y compris pour les petits montants. À cette fin, et dans l'objectif de faire profiter le grand public des innovations en matière de paiement, le Comité a mis en place un suivi de la mise en œuvre des engagements pris pour diminuer les obstacles tarifaires et techniques aux paiements par carte dès le premier euro. Il a également mis en place un dispositif de suivi du recours aux paiements sans contact et engagé une veille active des innovations en matière de paiements.

1 *http://www.economie.gouv.fr/files/files/PDF/Strategienationale_sur_moyens_de_paiement_102015.pdf*

Les actions menées au titre de ces priorités comportent toutes un volet important en matière de communication, tant auprès des entreprises que du grand public. À cet égard, deux dépliants, réalisés en collaboration avec le Comité consultatif du secteur financier et respectivement consacrés au virement SEPA et aux alternatives au paiement par chèque, ont été publiés en mai 2017. Ces actions se sont accompagnées, au plan européen, d'un suivi et de contributions aux travaux portant sur la dématérialisation de la chaîne des paiements.

1|4 La mise en place de l'Observatoire de la sécurité des moyens de paiement

La création de l'Observatoire de la sécurité des cartes de paiement (OSCP), par la loi du 15 novembre 2001 relative à la sécurité quotidienne, avait permis d'établir au niveau national une instance de concertation visant à renforcer la sécurité des opérations par carte.

Fort de la diversité d'origine de ses membres, représentant de manière équilibrée toutes les parties concernées par la sécurité des cartes de paiement, dans le domaine de l'offre (banques, systèmes de paiement par carte) comme dans celui de la demande (consommateurs, commerçants et entreprises) ainsi que les administrations publiques, l'OSCP a fortement contribué au cours de son existence au renforcement de la sécurité des paiements par carte en France, au travers notamment :

- de la collecte et de la publication annuelle de statistiques en matière de fraude aux cartes de paiement ;

- du renforcement de la sécurité des paiements sur internet par la promotion de l'adoption des dispositifs d'authentification forte du porteur de la carte lors du paiement ;

- de la sécurisation des paiements par carte ou par mobile en mode sans contact ;

- et de la sécurisation des solutions innovantes d'acceptation des paiements sur mobile.

Les travaux de l'OSCP ont ainsi permis de renforcer l'expertise de la Banque de France en matière de sécurité des cartes, et d'être force de proposition au niveau européen en ce qui concerne les exigences réglementaires et les cadres de surveillance applicables.

Prenant acte des succès de l'OSCP, tout en s'inscrivant dans la stratégie nationale des paiements lancée en octobre 2015 par le ministre de l'Économie et des Finances, la loi du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique a élargi le mandat de l'OSCP à l'ensemble des moyens de paiement scripturaux.

L' Observatoire de la sécurité des moyens de paiement (OSMP) reprend ainsi les missions de l'OSCP – suivi des mesures de sécurisation entreprises par les émetteurs, les commerçants et les entreprises, établissement de statistiques de la fraude et veille technologique en matière de moyens de paiement – sur un périmètre désormais élargi à l'ensemble des moyens de paiement scripturaux. Cet élargissement lui permettra notamment de réaliser les analyses de sécurité indispensables aux travaux conduits par le CNPS, en charge de veiller à la mise en œuvre de la stratégie nationale des paiements.

Les membres de l'OSMP nouvellement créé ont été nommés le 20 juin 2017 par arrêté du ministre de l'Économie et des Finances, en reconduisant le principe de l'équilibre de représentation entre l'offre et la demande, qui était déjà en vigueur au sein de l'OSCP. La Banque de France a été reconduite dans les fonctions de présidence (exercée par son gouverneur) et de secrétariat de ce nouvel Observatoire.

Les premiers travaux de l'OSMP ont porté sur l'harmonisation, entre les différents moyens de paiement, des méthodes de collecte des statistiques

de fraude. Son premier rapport annuel, publié le 18 juillet 2017 et disponible sur son site internet [2], présente ainsi un éclairage statistique sur la fraude aux paiements scripturaux en France en 2016.

Ses prochains travaux porteront notamment sur les modalités de mise en œuvre de l'authentification renforcée pour les moyens de paiement autres que la carte, telle que prévue par la DSP2.

1|5 La refonte du référentiel de sécurité du chèque

Le référentiel de sécurité du chèque (RSC), établi pour la première fois en 2005 par la Banque de France, décrit les objectifs de sécurité dont la Banque de France attend la mise en œuvre de la part des établissements intervenant au titre des différentes étapes de la gestion des opérations sur chèques. Il est complété par un questionnaire d'évaluation de la sécurité du chèque qui détaille les modalités de mise en œuvre de ces objectifs de sécurité.

La Banque de France a engagé, à la fin de l'année 2015, en lien avec la profession bancaire dans le cadre du Comité français d'organisation et de normalisation bancaires (CFONB), un processus de révision du RSC. Cette démarche s'inscrivait dans un contexte en forte évolution, sous l'effet de trois initiatives :

- la définition d'une stratégie nationale sur les moyens de paiement par le ministère de l'Économie et des Finances, encourageant la réduction de l'usage des chèques au profit des instruments de paiement électroniques ;

- les encouragements au maintien d'une vigilance forte en matière de maîtrise de risques de la filière chèque, tout en adaptant les contrôles pour mieux prendre en compte les points sensibles de la chaîne de paiement par chèque. Le chèque reste en effet le deuxième moyen de paiement le plus fraudé derrière la carte, alors qu'il n'est que le quatrième en termes d'utilisation (après la carte, le virement et le prélèvement) ;

- la volonté d'adaptation du RSC au format utilisé pour les autres référentiels de sécurité de moyens de paiement scripturaux établis par l'Eurosystème et la Banque de France.

Cette démarche a conduit à l'élaboration d'un référentiel révisé qui définit neuf objectifs de sécurité applicables au système de paiement par chèque, c'est-à-dire l'ensemble des processus afférents à la gestion du chèque au sein des établissements (cf. encadré 5).

Ce nouveau référentiel se décline dans un questionnaire d'autoévaluation, également révisé, à l'attention des établissements bancaires, permettant d'évaluer pour chacun des objectifs leur degré de conformité sur la base d'une analyse détaillée. Enfin, deux annexes, l'une dédiée à la description du système de paiement par chèque et l'autre constituée d'une table de correspondance avec la version précédente du référentiel, complètent le nouveau référentiel.

À l'issue d'une procédure de consultation publique de la Place conduite à l'été 2016, la Banque de France a publié le nouveau référentiel au deuxième semestre de cette même année sur son site internet [3]. Ce nouveau cadre de référence est entré en application le 1er janvier 2017, en vue d'une première déclaration annuelle des établissements attendue au cours du premier semestre 2018.

1|6 Les évolutions des cartes prépayées anonymes

Les cartes prépayées anonymes constituent une exception dans le paysage des moyens de paiement scripturaux, dans la mesure où elles permettent la préservation de l'anonymat du client lors des transactions. À ce titre, elles sont susceptibles d'être utilisées dans les circuits de blanchiment des capitaux ou de financement du terrorisme.

Les cartes prépayées relèvent du cadre réglementaire issu de la transposition de la deuxième directive

2 *www.observatoire-paiements.fr*

3 *https://www.banque-france.fr/stabilite-financiere/securite-des-moyens-de-paiement-scripturaux/surveillance-des-moyens-de-paiement-scripturaux*

Encadré 5

Les neuf objectifs de sécurité du nouveau référentiel de sécurité du chèque

1. Gouvernance et organisation

[…] La gouvernance de la sécurité vise à assurer que les mesures de sécurité sont en place, optimales et appropriées. Les acteurs [contribuant au système de paiement par chèque] doivent disposer d'un ensemble documentaire formalisé et régulièrement mis à jour définissant ce cadre de gouvernance et l'organisation de la sécurité du système de paiement par chèque, et couvrant l'ensemble des activités associées, y compris les activités externalisées.

2. Évaluation des risques

La gestion de la sécurité repose sur l'identification des actifs à protéger associée à une analyse des risques encourus ainsi qu'à la mise en place de mesures organisationnelles, techniques et procédurales en vue d'assurer cette protection. Elle prévoit une évaluation périodique des mesures déployées en vue de leur efficacité.

3. Contrôle et encadrement des risques

Les acteurs doivent mettre en œuvre des mesures de sécurité adéquates en vue d'encadrer les risques identifiés, en conformité avec la politique de sécurité de la filière.

4. Gestion des incidents et reporting

Les acteurs doivent disposer d'un système de surveillance des incidents relatif aux opérations et aux réclamations des clients qui permette un recensement exhaustif des incidents. Ce système de surveillance doit comprendre une procédure de remontée des incidents qui produise une information adéquate auprès des instances de gouvernance, ainsi qu'auprès des parties prenantes externes concernées.

5. Traçabilité - piste d'audit

Les acteurs doivent mettre en place un processus permettant une traçabilité destinée à alimenter une piste d'audit ininterrompue pour chacune des opérations couvertes par le système de paiement par chèque.

6. Sécurité physique du chèque

Les acteurs s'assurent de la sécurité des supports physiques du chèque tout au long de leur cycle de vie.

7. Sécurité des environnements des opérations

Les environnements physique et logique du système de paiement par chèque sont sécurisés, et permettent d'assurer la protection des supports physiques et logiques ainsi que des opérations exercées. Ils garantissent la qualité, la disponibilité et l'exploitabilité technique des éléments archivés.

8. Dispositif de surveillance des opérations

La surveillance des opérations vise à prévenir, détecter et bloquer les tentatives de paiement suspectées d'être d'origine frauduleuse. Cette surveillance doit être encadrée par une procédure formalisée définissant les règles et typologies d'alertes.

9. Sensibilisation des clients aux règles de sécurité

Les établissements veillent à la sensibilisation de leurs clients aux règles de vigilance relatives à la conservation d'une formule prémarquée, l'émission ou la réception d'un chèque, sa conservation et sa remise à l'encaissement.

européenne sur la monnaie électronique (DME2) par la loi n° 2013-100 du 28 janvier 2013. La loi prévoit à ce titre que seuls les émetteurs de monnaie électronique peuvent émettre et gérer les cartes prépayées, à savoir des établissements disposant d'un agrément d'établissement de monnaie électronique (EME) ou d'établissement de crédit délivré par l'autorité compétente nationale du pays de l'émetteur – en France, l'Autorité de contrôle prudentiel et de résolution (ACPR) – ou par les émetteurs agréés dans l'Espace économique européen bénéficiant du passeport européen.

Encadré 6

Qualification juridique des cartes prépayées et obligations de vigilance des émetteurs

La monnaie électronique est définie en droit français à l'article L315-1 du *Code monétaire et financier* comme étant « une valeur monétaire qui est stockée sous une forme électronique, y compris magnétique, représentant une créance sur l'émetteur, qui est émise contre la remise de fonds aux fins d'opérations de paiement […] et qui est acceptée par une personne physique ou morale autre que l'émetteur de monnaie électronique ». Concrètement, la monnaie électronique est le plus souvent utilisable au moyen de cartes de paiement dites « prépayées », qui peuvent soit servir à faire des achats en circuit fermé, soit être utilisées comme toute autre carte de paiement. Ces cartes prépayées sont le plus souvent adossées aux systèmes de paiement par carte internationaux tels que Visa ou MasterCard.

Les établissements dits de monnaie électronique, au même titre que les établissements de crédit, sont assujettis à la réglementation relative à lutte contre le blanchiment des capitaux et le financement du terrorisme, notamment aux obligations d'identification et vérification de l'identité du client ainsi que de connaissance de celui-ci. Toutefois, une dérogation à ces obligations est prévue au 5° de l'article R561-16 du *Code monétaire et financier* dans les conditions suivantes :

- la monnaie électronique est utilisée uniquement pour l'acquisition de biens et de services ;
- la capacité maximale du support n'est pas supérieure à 250 euros ;
- si le support peut être rechargé, les paiements sont limités à 250 euros par période de trente jours et est utilisable uniquement sur le territoire national ;
- le support ne peut être chargé au moyen de monnaie électronique elle-même anonyme ou d'espèces (sauf dans le cas où la monnaie électronique ne peut être utilisée que dans un réseau d'acceptation limité ou pour un éventail limité de biens ou de services, comme c'est le cas par exemple pour les cartes cadeaux).

Ces conditions de dérogation aux obligations de vigilance, déjà durcies par le décret du 10 novembre 2016 relatif à la lutte contre le financement du terrorisme adopté à la suite des attentats de Paris, pourraient être restreintes dans le cadre de la transposition de la future cinquième directive européenne de lutte anti-blanchiment.

En outre, les opérations de remboursement unitaires en espèces ou de retrait en espèces d'un montant supérieur à 100 euros sont sujettes aux obligations de vigilance précitées.

La monnaie électronique émise dans le cadre de cette dérogation est appelée monnaie électronique anonyme. Ainsi, par exemple, une carte prépayée de monnaie électronique non rechargeable peut être achetée (le plus souvent sur internet ou auprès d'un commerçant de proximité), sans que l'émetteur de celle-ci ait à se conformer aux obligations d'identification/vérification de l'identité du client, dès lors que le montant préchargé n'excède pas 250 euros.

Les EME et les établissements de crédit sont soumis aux obligations en matière de lutte contre le blanchiment des capitaux et le financement du terrorisme (LCB-FT) de l'État membre dans lequel ils sont établis, sous le contrôle de l'autorité compétente de cet État membre.

En réponse aux risques que représentent ces instruments de paiement en termes de blanchiment des capitaux et de financement du terrorisme, la Banque de France a contribué, aux côtés des autres autorités concernées dont l'ACPR qui est en charge du contrôle du respect des obligations LCB-FT par les organismes financiers établis en France, et des pouvoirs publics français, au renforcement des exigences applicables :

• au niveau européen, par des amendements proposés à la quatrième directive de lutte contre le blanchiment des capitaux et le financement du terrorisme concernant l'abaissement des seuils de la monnaie électronique dite « anonyme » à 150 euros (contre 250 euros dans le texte initial de la directive), la limitation des remboursements en espèces sans vérification de l'identité du porteur à 50 euros (contre 100 euros ou encore l'identification du porteur en cas de paiement sur internet ;

• au niveau national, par l'adoption de mesures restrictives quant à l'émission et l'utilisation de cartes prépayées (anonymes ou non), notamment la limitation de la valeur monétaire maximale stockée à 10 000 euros, la limitation des capacités de chargement en espèces ou en monnaie électronique à 1 000 euros par mois et la limitation des opérations de retrait ou de remboursement en espèces à 1 000 euros par mois.

2 Le bilan de la surveillance des moyens de paiement scripturaux

2.1 Le bilan de la migration *post* SEPA

Conformément aux dispositions du règlement UE n° 260/2012 qui prévoyaient un délai supplémentaire pour les produits dits « de niche », la seconde phase de la migration vers les moyens de paiement SEPA s'est achevée pour la France en février 2016 avec le remplacement du titre interbancaire de paiement (TIP) et du télérèglement par le prélèvement SEPA *Core* pour le premier et le prélèvement SEPA *Core* ou interentreprises selon la nature du payeur pour le second.

Le suivi de cette migration, assuré par la Banque de France au titre du secrétariat du Comité national SEPA puis, à compter de 2016, du CNPS, a mis en exergue les contraintes spécifiques liées à l'utilisation du prélèvement SEPA Interentreprises, plus précisément l'obligation pour le payeur d'informer préalablement à la première transaction son établissement bancaire de la signature d'un mandat de prélèvement. Ces contraintes opérationnelles ont été sources de difficultés pour les créanciers qui avaient choisi cet instrument de paiement, en particulier ceux de la sphère publique et sociale, et ont entraîné d'importants taux de rejet pour certains d'entre eux.

Pour cette raison, plusieurs créanciers ont décidé en 2017 de remplacer le prélèvement SEPA interentreprises par le prélèvement SEPA *Core*. Cette nouvelle migration, coordonnée par le CNPS, s'est déroulée avec succès durant l'été 2017. Elle a ainsi permis de fluidifier le processus de paiement par prélèvement et d'améliorer l'efficacité générale des paiements pour les usagers concernés [4].

2.2 Contribution de la Banque de France à la procédure d'agrément 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 L141-4 du *Code monétaire et financier*, sur les moyens techniques, informatiques et organisationnels relatifs à la sécurité des moyens de paiement pour les activités envisagées par les sociétés sollicitant l'agrément. Cette consultation aboutit à la préparation d'un avis de la Banque de France.

4 Pour plus d'informations sur le sujet, le premier rapport d'activité du CNPS est disponible à l'adresse suivante : *https://www.banque-france.fr/sites/default/files/media/2017/07/18/cnps_2017_web.pdf*.

Entre le 1er janvier 2015 et le 31 décembre 2017, la Banque de France a ainsi délivré à l'ACPR 46 avis positifs, portant sur :

- 11 procédures d'agrément au statut d'établissement de paiement ;
- 3 procédures d'agrément au statut d'établissement de monnaie électronique ;
- 24 procédures d'exemption d'agrément au statut d'établissement de paiement ;
- 1 procédure d'exemption d'agrément au statut d'établissement de monnaie électronique ;
- 1 procédure d'exemption d'agrément au double statut d'établissement de paiement et d'établissement de monnaie électronique ;
- 3 procédures d'extension d'agrément à d'autres services de paiement portant sur des établissements de paiement ;
- 3 procédures d'extension à la fourniture de services de paiement portant sur des établissements de monnaie électronique.

Pour mémoire, ces établissements restent ensuite assujettis à la surveillance de la Banque de France, comme tout prestataire de services de paiement opérant en France [5]. Plus particulièrement, ils sont soumis à l'ensemble des obligations déclaratives auprès de la Banque de France, en matière de statistiques annuelles de fraude mais également de description des évolutions de leurs dispositifs de gestion des risques concernant les services de paiement fournis. Ils peuvent par ailleurs faire l'objet de contrôles sur place.

2|3 La participation aux actions de surveillance de l'Eurosystème sur les cartes de paiement

En février 2015, la BCE a publié une version actualisée du guide d'évaluation des systèmes de paiement par carte [6], visant à intégrer les recommandations du forum européen sur la sécurité des moyens de paiement de détail du 31 janvier 2013 relatives à la sécurité des paiements sur internet, lesquelles abordent différents aspects de la sécurité des paiements sur internet autour des thèmes suivants :

- l'environnement général de contrôle et de sécurité (gouvernance, dispositifs d'évaluation et d'atténuation des risques, suivi et déclaration des incidents, traçabilité) ;
- les mesures de contrôle et de sécurité spécifiques pour les paiements sur internet (recours à l'authentification forte du payeur, suivi des opérations, protection des données sensibles, fixation de limites, fourniture d'informations aux clients sur les opérations) ;
- l'éducation du client et les modalités de communication entre ce dernier et l'établissement émetteur de sa carte de paiement.

Ces recommandations ont ainsi introduit un renforcement des exigences applicables aux systèmes de paiement par carte, qui justifiait de procéder à une nouvelle évaluation de la conformité de l'ensemble des systèmes opérant en Europe (cf. encadré *infra*).

Le premier exercice d'évaluation des systèmes de paiement par carte ayant été conclu en 2014, soit un an seulement avant l'entrée en application du nouveau guide d'évaluation, l'Eurosystème a choisi de limiter ce second exercice aux exigences nouvelles et à celles qui avaient fait l'objet d'évolutions. À cette fin, les banques centrales nationales du Système européen de banques centrales ont été appelées à évaluer individuellement chacun des systèmes opérant dans leurs pays respectifs, et à assister les banques centrales chargées de coordonner l'évaluation des systèmes internationaux [7]. En parallèle de l'évaluation des six systèmes de paiement par carte français [8], un nombre record en Europe, la Banque de France est l'une des

5 Cf. le rapport de surveillance 2014 : *https://www.banque-france.fr/sites/default/files/medias/documents/rapport-surveillance-moyens-paiement-et-infrastructures-marches-financiers_2014_fr.pdf* – (paragraphe 4.1.2)

6 *http://www.ecb.europa.eu/pub/pdf/other/guideassessmentcpsagainstoversightstandards201502.en.pdf*

7 Soit la BCE pour les systèmes de paiement par carte American Express et Visa, et la Banque nationale de Belgique pour MasterCard.

8 Soit le système de paiement interbancaire Cartes Bancaires, ainsi que les cinq systèmes de paiement privatifs BNP Paribas Personal Finance, Cofidis, Crédit Agricole Consumer Finance, Franfinance, Oney Bank.

Encadré 7

Principales mesures de sécurité introduites par les recommandations de la Banque centrale européenne dans le guide d'évaluation

Standard 3.1 – Gestion de la sécurité

- Analyse des risques et politique de sécurité du système de paiement par carte cohérentes entre elles et révisées régulièrement
- Veille technologique et sécuritaire permanente permettant d'actualiser le profil de risque
- Dispositif de remontée, de classification et de suivi des incidents
- Processus formalisé de gestion des évolutions
- Politique restrictive de gestion des accès physiques et logiques aux infrastructures
- Protection des données sensibles échangées lors des transactions, basée sur des techniques cryptographiques avancées
- Plan de continuité en cas de compromission de données sensibles

Standard 3.2 – Fabrication et distribution des cartes

- Exigences minimales de sécurité applicables aux cartes et aux terminaux de paiement
- Procédure de communication sécurisée des éléments sensibles d'authentification (code PIN, numéro de téléphone pour l'envoi des mots de passe à usage unique, etc.)
- Enrôlement des porteurs dans un dispositif d'authentification forte pour les paiements sur internet

Standard 3.3 – Transactions

- Limites de validité des cartes et des données d'authentification
- Spécifications de sécurité propres aux différents modes d'utilisation des cartes en fonction de leur niveau de risque
- Dispositif de détection des opérations non autorisées ou frauduleuses
- Mesures de limitation de la fraude (plafonds de paiement par canal, mécanisme de mise en opposition des cartes, etc.)
- Mécanismes incitatifs à l'attention des participants au système de paiement par carte pour limiter la fraude (par exemple, transfert de responsabilité à l'émetteur en cas de recours à l'authentification forte)

rares banques centrales à participer aux travaux d'évaluation des trois systèmes internationaux visés par cette démarche.

Les évaluations conduites auprès des six systèmes de paiement par carte français ont permis de mettre en évidence un degré de conformité élevé aux exigences du cadre de surveillance, qui a pu être facilité par les actions conduites dès 2009 par l'OSCP pour renforcer la sécurité des paiements sur internet, lesquelles ont préfiguré les exigences adoptées par la suite par les autorités européennes.

2|4 La vérification de la sécurité et du bon fonctionnement du chèque et des paiements en ligne

Dans l'exercice de sa mission de surveillance des moyens de paiement scripturaux, conformément à l'article L141-4 du *Code monétaire et financier*, la Banque de France peut procéder à toute expertise utile concernant les moyens de paiement ou les dispositifs techniques qui leur sont associés. Des missions de contrôle sur place, conduites par l'Inspection générale de la Banque de France, sont à ce titre diligentées sur une base régulière. Ainsi, deux séries de missions d'inspection sur place ont été conduites sur la période de 2014 à 2016 au sein de plusieurs groupes bancaires français.

Mission de vérification de la sécurité et du bon fonctionnement du système de paiement par chèque

Cette série de missions s'est déroulée au cours du quatrième trimestre 2014 et avait pour objectif d'évaluer la sécurité et le bon fonctionnement de la gestion des activités liées au chèque au sein de plusieurs groupes et établissements bancaires français sélectionnés sur la base de leur taille et de leur représentativité. Parmi les thèmes examinés dans le cadre de ces missions ont figuré notamment l'organisation de la filière chèque (fabrication, distribution, remise à l'encaissement et traitement du chèque) et l'identification et le suivi de la fraude sur ce moyen de paiement.

Les processus liés au chèque, qui sont aujourd'hui largement externalisés, sont ressortis globalement bien maîtrisés avec un pilotage et un suivi des prestataires assurés de manière satisfaisante par les établissements. Dans l'ensemble, les établissements sont apparus sensibilisés à la lutte contre la fraude au chèque avec des structures internes et des outils dédiés à son recensement et son analyse. Plusieurs axes d'améliorations ont été cependant proposés, notamment sur le renforcement des dispositifs de contrôle interne et, sur l'amélioration de la qualité des statistiques de fraude déclarées auprès de la Banque de France.

Les enseignements de cette série de missions ont par ailleurs permis d'alimenter les travaux de refonte du référentiel de sécurité du chèque (cf. section 1|5).

Mission de vérification de la conformité aux orientations de l'Autorité bancaire européenne relatives à la sécurité des paiements sur internet

Cette seconde série de missions, menée en juin et juillet 2016, visait à s'assurer de la conformité des processus d'administration et de gestion des paiements sur internet au regard des orientations de l'Autorité bancaire européenne (ABE) entrées en vigueur au 1er août 2015. Ces orientations couvrent deux thématiques principales : l'environnement général de contrôle et de sécurité, d'une part, et les mesures de contrôle et de sécurité spécifiques pour les paiements sur internet, d'autre part. Cette série de missions a été réalisée auprès d'établissements aux profils différenciés tant en termes de taille que de type de clientèle ou encore de services offerts.

À l'issue de ces missions, il ressort que la conformité des processus aux orientations de l'ABE en matière de sécurité des paiements sur internet est globalement satisfaisante. Les établissements sont apparus attentifs à la fraude et réactifs pour renforcer la sécurité des dispositifs en place. Toutefois, alors que le périmètre des données sensibles en matière de paiement s'élargit en ne se limitant plus aux seuls identifiants bancaires (numéro de carte, IBAN) un point de vigilance particulier est à souligner en ce qui concerne la protection d'autres données, telles les numéros de téléphone ou courriels par exemple, qui concourent désormais à la sécurité des opérations de paiement et doivent donc être protégées contre des attaques par hameçonnage (ou *phishing*).

La mission a également permis de souligner les développements réalisés en matière de sécurisation des opérations : des solutions d'authentification forte du client ont ainsi été déployées par tous les établissements audités pour sécuriser l'accès à l'initiation de paiements sur internet ainsi que pour l'accès aux données sensibles de paiement.

2|5 Le bilan de la surveillance des titres spéciaux de paiement dématérialisés

Dans le cadre de la mission de surveillance de la sécurité des titres spéciaux de paiement dématérialisés (TSPD) et des chèques emploi service universels (CESU) qui lui a été confiée par la loi n° 2013-100 du 28 janvier 2013, la Banque de France a mis en application à compter de l'exercice 2014 le dispositif annuel de suivi des émetteurs de titres, fondé sur la collecte de questionnaires d'autoévaluation des émetteurs sur leur conformité aux objectifs de sécurité applicables, ainsi que des données statistiques opérationnelles et de fraude [9].

Le bilan des trois premiers exercices de surveillance unifiée pour les TSPD et les CESU, couvrant les années 2014 à 2016, est le suivant :

- en termes de volume d'émission et d'utilisation, ces titres représentent une part marginale (0,004 %) à l'échelle des flux de transactions sur l'ensemble des moyens de paiement scripturaux, soit environ 1,2 milliard d'euros de flux de paiement annuels pour ces titres contre par exemple 499 milliards d'euros pour les paiements par carte ou 1 077 milliards d'euros pour le chèque en 2016 (cf. graphique 7a) ;

9 Cf. le rapport de surveillance 2014 : *https://www.banque-france.fr/sites/default/files/medias/documents/rapport-surveillance-moyens-paiement-et-infrastructures-marches-financiers_2014_fr.pdf*

• ces titres sont soumis à des conditions d'utilisation restrictives qui en limitent l'attractivité pour les fraudeurs. Ainsi, le montant total de la fraude observé en 2016 est de 151 euros, après 27 euros en 2015 et 31 629 euros en 2014 (marqué par un cas exceptionnel de fraude par malveillance interne au sein d'un dispositif d'aide sociale sur les CESU). Le taux de fraude sur ces titres est par conséquent extrêmement faible au regard des taux observés sur les autres moyens de paiement ; par exemple, le taux de fraude sur les TSPD est dix fois inférieur à celui du virement, qui est pourtant l'instrument de paiement proportionnellement le moins fraudé [10] (cf. graphique 7b) ;

• concernant la conformité des émetteurs aux objectifs de sécurité des référentiels, les informations fournies par les émetteurs permettent de justifier d'un niveau de conformité des TSPD et CESU globalement satisfaisant sur l'ensemble des objectifs de sécurité.

Au regard de ces constats, et en vue d'assurer une activité de surveillance proportionnée au niveau de risque réel supporté par ces titres, les modalités de collecte ont été allégées à compter de l'exercice 2017, selon les orientations suivantes :

• une réduction de la fréquence de la collecte d'autoévaluation sur les objectifs de sécurité : compte tenu du degré satisfaisant de maturité observé sur les objectifs de sécurité et du niveau de fraude très limité sur les deux catégories de titres, l'autoévaluation sera désormais conduite sur une période triennale. Dans ce cas de figure, seuls les nouveaux établissements émetteurs sont invités à fournir leur autoévaluation en dehors des années de collecte ;

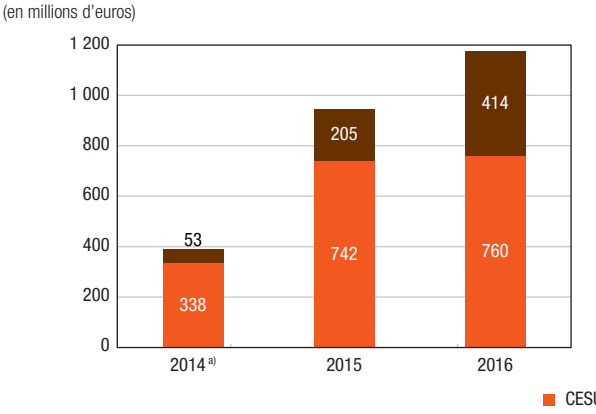
• un suivi statistique plus fréquent du développement de la fraude, permettant de réagir rapidement en cas de détérioration du niveau de sécurité : dans cette logique, les données relatives au nombre de transactions, de cas de fraude, de tentatives de fraude et les montants correspondants seront collectées trimestriellement, et non plus annuellement ;

• un maintien à l'identique, sur une base annuelle, de la collecte des autres données statistiques sur les activités d'émission de titres : le maintien de cette collecte annuelle, portant notamment sur le nombre de financeurs et de bénéficiaires ainsi que sur les volumes et montants des titres émis dans l'année et en circulation à fin d'année, est nécessaire

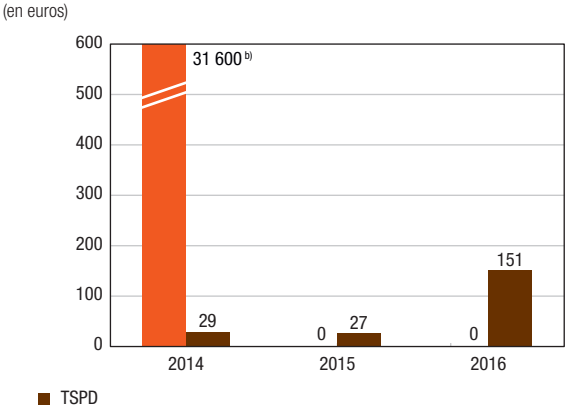
10 Cf. rapport annuel 2016 de l'Observatoire de la sécurité des moyens de paiement : *www.observatoire-paiements.fr*

G7 Utilisation des CESU et des TSPD

a) Montant des paiements



b) Montant de la fraude



a) Données partielles en 2014
b) Cas exceptionnel de fraude par malveillance interne au sein d'un dispositif d'aide sociale sur les CESU.
Source : Banque de France.

en vue d'assurer un suivi régulier du développement de l'émission de ces titres (notamment pour les TSPD, avec la migration des titres papier).

Enfin, dans l'hypothèse où les collectes statistiques trimestrielles viendraient à montrer une augmentation significative de la fraude, la Banque de France privilégierait dans un premier temps son dispositif de surveillance permanent afin d'agir rapidement auprès de l'émetteur concerné (échanges bilatéraux, recommandations), tout en se réservant la possibilité de réactiver la collecte sur les objectifs de sécurité si le phénomène n'était pas isolé, celle-ci faisant l'objet de réunions bilatérales sur les résultats obtenus.

2|6 La surveillance des monnaies locales complémentaires

Les monnaies locales complémentaires, émises au niveau de collectivités territoriales en vue de promouvoir les échanges économiques entre acteurs locaux, relèvent du statut de « titres de monnaies locales complémentaires » au sens du *Code monétaire et financier*. Ce dernier dispose que ces titres sont émis par des entreprises poursuivant une utilité sociale au sens de la loi du 31 juillet 2014, et dont l'émission de tels titres est l'unique objet social.

Afin de poursuivre leur activité, les entreprises émettrices ou gestionnaires de titres de monnaies locales complémentaires doivent bénéficier d'un statut de prestataire de service de paiement. Le régime d'agrément est toutefois variable selon le support utilisé pour l'émission de monnaies locales, avec pour chacun des cas des possibilités d'exemption.

Les titres de monnaies locales complémentaires étant considérés comme des moyens de paiement, la Banque de France est chargée de veiller à leur sécurité dès lors qu'ils sont émis sous forme scripturale. Elle produit également, dans le cadre de l'instruction des demandes d'agrément ou d'exemption déposées auprès de l'ACPR, des avis relatifs à la sécurité de ces activités.

2|7 L'analyse des risques liés au développement des crypto-actifs

Les actifs cryptographiques, tels que le bitcoin, l'ether ou le ripple, ne sont pas considérés comme des monnaies alternatives. Ils ne remplissent pas les trois fonctions dévolues à la monnaie (unité de compte, intermédiaire des échanges et réserve de valeur), et ne répondent pas non plus à la définition des moyens de paiement ni à celle de la monnaie électronique au sens du *Code monétaire et financier*.

La Banque de France a publiquement alerté, en particulier dans un *Focus* paru le 5 mars 2018 [11], sur les risques associés aux crypto-actifs, dans un contexte de forte progression de la valorisation globale de ces actifs, et contribue activement aux réflexions des autorités nationales, européennes et internationales sur les pistes de réglementation.

Les risques liés au caractère spéculatif des crypto-actifs

La convertibilité des crypto-actifs dans différentes monnaies ayant cours légal n'est garantie par aucun organisme centralisé. Ainsi, les investisseurs ne peuvent récupérer leurs fonds en devises que si d'autres utilisateurs désirent acquérir les mêmes crypto-actifs. De ce fait, le cours d'un crypto-actif peut à tout moment s'effondrer si les investisseurs voulant dénouer leurs positions ne trouvent pas d'acquéreurs et se retrouvent détenteurs de portefeuilles illiquides.

Dans le cas particulier du bitcoin, le processus d'émission d'unités, qui est uniquement dépendant d'une puissance de calcul informatique, est plafonné dans le temps. Cette limitation nourrit un phénomène de pénurie qui, face à la forte demande induite principalement pour le motif de spéculation, entraîne de très fortes fluctuations de cours.

11 *https://www.banque-france.fr/sites/default/files/medias/documents/focus-16_2018_03_05_fr.pdf*

Une diversification des usages qui expose les investisseurs à des risques de perte financière accrus

Les crypto-actifs suscitent un intérêt croissant en dehors de leurs communautés initiales, c'est-à-dire auprès des utilisateurs et des commerçants n'ayant pas un rôle opérationnel dans le réseau d'émission et de gestion de ces actifs (par exemple, « non-mineurs » [12] de crypto-actifs). Cela entraîne le développement de nombreux services, qui se structurent en s'inspirant des services existant dans la sphère financière traditionnelle.

Ainsi, dans le domaine des infrastructures de marché, des plateformes d'échange permettant l'achat et la vente de crypto-actifs contre de la monnaie ayant cours légal (EUR, USD, etc.) ont été créées. Ces plateformes permettent à des utilisateurs n'ayant pas participé au processus de création d'acquérir des crypto-actifs, ou de convertir en monnaie ayant cours légal des crypto-actifs reçus en paiement. Dans le sillage de cette activité de plateforme d'échange contre monnaie ayant cours légal, se multiplient également des prestations de services en matière de conservation des crypto-actifs, qui sont assimilables à des activités de dépositaires.

Liés à ces échanges, se développent des services en matière d'information financière et de fournitures de données, de conseil en investissement ou encore de *trading*. Ces activités favorisent la création d'instruments d'investissement adossés aux crypto-actifs, comme la constitution de fonds ou la mise en place d'instruments dérivés, à l'instar des initiatives du *Chicago Board Options Exchange* ou du *Chicago Mercantile Exchange*.

L'activité de financement a également tiré parti du développement des crypto-actifs avec les ICO, pour *Initial Coin Offering*. Les ICO constituent la transposition en crypto-actifs du concept de financement participatif : dans ce type de montage, les internautes qui contribuent à un projet par l'apport de fonds (en crypto-actifs ou en monnaies ayant cours légal) reçoivent, en contrepartie, des actifs digitaux (ou *tokens*). En pratique, ces *tokens* représentent une forme d'intérêt économique dans le projet. Ils offrent à leurs détenteurs certains droits, comme celui d'utiliser en primeur la plateforme ou l'application financée (comme dans le financement participatif classique), de recevoir une partie des bénéfices générés par l'entreprise ou d'exercer un droit de vote (comme des actions). La gestion des *tokens* émis lors des ICO étant elle-même assurée au travers de la *blockchain* utilisée pour l'ICO, elle repose sur des mécanismes d'échange en tous points similaires à ceux des crypto-actifs. Ils s'apparentent ainsi à une forme supplémentaire de crypto-actifs, enrichis de droits spécifiques (droit d'accès privilégié au projet financé, droit de vote, etc.). Les limites et les risques des crypto-actifs décrits ici s'appliquent donc aussi à ces *tokens*.

Des mécanismes anonymes qui favorisent le financement du terrorisme et d'activités criminelles ainsi que le contournement des règles relatives à la lutte contre le blanchiment des capitaux

L'anonymat, qui caractérise les mécanismes d'émission et de transfert de la plupart des crypto-actifs, favorise avant tout un risque d'utilisation de ces actifs à des fins criminelles (vente sur internet de biens ou services illicites) ou à des fins de blanchiment ou de financement du terrorisme.

En France, l'organisme Tracfin (Traitement du renseignement et action contre les circuits financiers clandestins) identifie l'utilisation de crypto-actifs, notamment le bitcoin, comme étant à l'origine d'un risque spécifique en matière de blanchiment des capitaux et de financement du terrorisme.

12 On désigne sous le terme de « mineurs » les participants directs au réseau d'émission et de gestion des transactions en crypto-actifs, chargés d'exécuter un algorithme assurant la validation et l'historisation des opérations au travers d'un registre dit « distribué ».

Des cyber-risques importants sur la détention des avoirs en crypto-actifs

Il existe des risques avérés de piratage des portefeuilles électroniques qui permettent le stockage des crypto-actifs. Dans ce contexte, les détenteurs n'ont aucun recours en cas de vol de leurs avoirs par des pirates informatiques. Les épisodes répétés de fraudes importantes (piratage de Coincheck en janvier 2018 pour 534 millions de dollars, faillite retentissante en 2015 de la première plateforme mondiale d'échange de bitcoin, MtGox [13]), illustrent la vulnérabilité de l'écosystème des crypto-actifs et le niveau élevé des risques associés, en l'absence de mécanismes de garantie.

Un coût environnemental inhérent au fonctionnement des crypto-actifs

Les activités informatiques de validation des transactions en crypto-actifs ont également un impact environnemental lié aux ressources énergétiques mobilisées : pour la validation d'une seule opération en bitcoin, la consommation d'électricité était estimée en décembre 2017 à 215 kWh. Cette consommation énergétique fait l'objet d'une réévaluation constante, à la hausse, en raison de la concurrence accrue associée à l'élargissement du réseau de validation des opérations.

13 À la suite d'une fraude interne ayant entraîné le détournement de 650 000 bitcoins pour une contrevaleur d'environ 360 millions de dollars.

Encadré 8

Les pistes de réglementation explorées par les autorités publiques

Une réglementation des activités liées aux crypto-actifs est souhaitable pour quatre motifs principaux : la lutte contre le blanchiment des capitaux (LCB) et le financement du terrorisme (FT) – qui apparait hautement prioritaire –, la protection des investisseurs, la préservation de l'intégrité des marchés, y compris face au cyber-risque, et enfin, en cas de poursuite de l'essor de ces activités, les préoccupations de stabilité financière.

La Banque de France et l'Autorité de contrôle prudentiel et de résolution (ACPR) préconisent un élargissement de l'encadrement des prestations de service associées aux crypto-actifs de manière à couvrir deux champs

1. Réglementer les services offerts à l'interface entre la sphère réelle et les crypto-actifs

L'activité des plateformes de conversion des crypto-actifs contre monnaie ayant cours légal, qui jouent le rôle d'intermédiaire entre acheteur et vendeur, est considérée comme un service de paiement nécessitant un agrément de prestataire de service de paiement. Toutefois, cette exigence découle de la gestion pour le compte de tiers de comptes tenus et libellés dans une monnaie ayant cours légal, et pas de la prestation associée aux crypto-actifs.

Au-delà de cette approche, la Banque de France et l'ACPR préconisent un élargissement de l'encadrement réglementaire applicable aux prestations associées aux crypto-actifs, par la mise en place d'un statut de prestataire de services en crypto-actifs.

Cette évolution réglementaire pourrait s'inscrire dans le prolongement de la révision de la quatrième directive de lutte contre le blanchiment des capitaux et le financement du terrorisme en cours d'adoption par l'Union européenne (dite « cinquième directive LCB-FT »). Cette directive prévoit en effet d'assujettir à cette réglementation les acteurs proposant i) des services d'échange de crypto-actifs contre de la monnaie ayant cours légal et ii) la conservation pour le compte de leurs clients des clés cryptographiques privées permettant de détenir, stocker ou transférer les crypto-actifs.

Un statut de prestataire de services en crypto-actifs permettrait, au-delà de la lutte contre le blanchiment et le financement du terrorisme qui constitue une priorité, de les soumettre à des règles portant notamment sur la sécurité des opérations et sur la protection de la clientèle. Ce statut pourrait également couvrir les services concernant les transactions entre crypto-actifs.

.../...

2. Encadrer les placements en crypto-actifs

L'encadrement réglementaire des prestataires de services en crypto-actifs pourrait être complété par une limitation de la possibilité pour certaines entreprises régulées (banques, assurances, sociétés de gestion, etc.) d'intervenir sur ces crypto-actifs. Il s'agirait d'abord d'interdire les activités de dépôts et prêts en crypto-actifs. Concernant les produits d'épargne, la question se pose de l'interdiction de toute commercialisation dans des véhicules collectifs à destination du grand public, pour réserver ces véhicules aux investisseurs les plus avertis. Ces produits devraient par ailleurs être assujettis à des règles strictes de protection de la clientèle. Enfin, pour les placements pour compte propre des entités régulées, un strict encadrement de ces placements, par exemple en déduisant la totalité de ces investissements des fonds propres, devrait être envisagé. Ces dispositions supposent une évolution des textes législatifs nationaux ou européens.

Pour sa part, l'Autorité des marchés financiers (AMF) considère que l'offre de dérivés sur les cryptomonnaies nécessite un agrément et ne doit pas faire l'objet de publicité par voie électronique. Par ailleurs, dans le prolongement de sa consultation publique sur les *Initial Coin Offering* (ICO), l'AMF a décidé de poursuivre le travail relatif à la définition d'un cadre juridique spécifique aux ICO prévoyant les garanties appropriées, notamment en matière d'information, qui seront nécessaires pour ce nouveau type d'offres. Ce travail sera mené en coordination avec les autres autorités publiques concernées.

Afin d'assurer une meilleure efficacité de la réglementation, il apparait souhaitable de développer une coordination européenne et internationale

Compte tenu du caractère dématérialisé des crypto-actifs et de l'utilisation de technologies liées au monde de l'internet qui facilitent la fourniture de services de façon transfrontalière, l'hétérogénéité des règlementations nationales empêche une pleine maîtrise des risques induits.

Ainsi, il apparait nécessaire aujourd'hui de porter le débat sur la régulation des crypto-actifs au niveau international. Le 7 février 2018, les ministres de l'Économie et des Finances et les banquiers centraux français et allemands ont saisi le G20 à cet effet.

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 systèmes de paiement 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 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
PFMI	*Principles for Financial Market Infrastructures* – principes pour les infrastructures des marchés financiers

SCT	*SEPA Credit Transfer* – virement SEPA
SDD	*SEPA Direct Debit* – prélèvement SEPA
SEPA	*Single Euro Payments Area* – espace unique de paiement en euros
SEPA.EU	Système de paiement de détail à vocation paneuropéenne
SPIS	Systèmes de paiement d'importance systémique
SSS	*Securities settlement system* – Système de règlement-livraison de titres
STEP2-T	Système de paiement de détail
STET	Systèmes Technologiques d'Échange et de Traitement – société gérant le système de paiement de détail CORE(FR)
SWIFT	*Society for Worldwide Interbank Financial Telecommunication*
T2S	TARGET2-*Securities*
TARGET2	Système de transferts express automatisés transeuropéens, système de paiement à règlement brut en temps réel (RBTR ou RTGS) en euro, développé et géré par l'Eurosystème

Des précisions complémentaires peuvent être obtenues sur le glossaire de la Banque des règlements internationaux : *http://www.bis.org/cpmi/publ/d00b.htm*

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

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

Directeur de la rédaction
Emmanuelle Assouan
Directeur des Systèmes de paiement
et Infrastructures de marché
Banque de France

Traduction et réalisation
Studio Création
Direction de la Communication

Imprimeur
Banque de France – SG - DISG

Dépôt légal
Mars 2018

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