E. Numérisation

Les technologies disruptives et les modèles d'entreprise innovants ont une incidence de plus en plus importante sur la fourniture de services financiers. Ces dernières années, les nouveaux venus dans le domaine de la haute technologie se sont fortement concentrés sur certains segments, dont les paiements, la notation de crédit et le conseil en investissement automatisé. Les méthodes et les plateformes innovantes permettent à ces nouveaux venus de répondre directement aux besoins changeants des utilisateurs finaux, par exemple la facilité d'utilisation, le traitement immédiat et le rapport coût/efficacité. Le présent chapitre expose plus en détail deux tendances : les innovations dans le secteur des paiements grâce à l'introduction de l'Open Banking, et les stablecoins (crypto-monnaies adossées à des devises) mondiaux. La numérisation croissante des services financiers a également pour conséquence que les risques informatiques et les cyber-risques doivent être suivis de près. Les évolutions dans ce domaine sont traitées dans le dernier paragraphe.

1. Open Banking

La deuxième directive européenne sur les services de paiement (PSD2)[1], qui a été transposée en droit belge par la loi du 11 mars 2018, porte sur des innovations dans le secteur des paiements et impose aux prestataires de services de paiement gestionnaires de comptes (comme les banques) de procéder à l'ouverture de leur infrastructure de comptes de paiement en ligne (*Open Banking*). Cela permet aux prestataires de services d'initiation de paiement et aux prestataires de services d'information sur les comptes (tant les banques et les établissements de paiement que les établissements de monnaie électronique) d'entrer sur le marché des services de paiement.

L'ouverture de cette infrastructure des comptes de paiement s'accompagne d'exigences de sécurité strictes qui doivent pouvoir être respectées par tous les prestataires de services de paiement concernés (banques, établissements de paiement et établissements de monnaie électronique). Ces exigences de sécurité sont contenues dans le règlement délégué (UE) 2018/389 de la Commission[2], qui est entré en vigueur le 14 septembre 2019.

Le secteur bancaire n'a pas attendu l'entrée en vigueur de ces exigences de sécurité pour développer ces nouveaux services de paiement sur le marché belge. Quelques banques belges offrent déjà la possibilité à la fois de consulter par leurs propres canaux les comptes de paiement détenus auprès d'autres banques belges et d'initier des ordres de paiement à partir de ces autres comptes de paiement. En outre, en 2019, la Banque a octroyé à sept établissements de paiement et à deux établissements de monnaie électronique un agrément (ou une extension de celui-ci) en tant que prestataires de services d'initiation de paiement et/ou de prestataires de services d'information sur les comptes.

1 Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le règlement (UE) n° 1093/2010, et abrogeant la directive 2007/64/CE.

2 Règlement délégué (UE) 2018/389 de la Commission du 27 novembre 2017 complétant la directive (UE) 2015/2366 du Parlement européen et du Conseil par des normes techniques de réglementation relatives à l'authentification forte du client et à des normes ouvertes communes et sécurisées de communication.

L'ouverture obligatoire des comptes de paiement par des prestataires belges de services de paiement gestionnaires de comptes (principalement des banques) s'est surtout concrétisée au moyen d'une interface dédiée, élaborée par les banques concernées. À la demande de celles-ci et après vérification du respect des exigences légales, la Banque a exempté un certain nombre de ces interfaces dédiées de l'obligation de disposer d'un mécanisme de secours conformément au règlement délégué (UE) 2018/389. Un grand nombre d'autres banques devraient adresser à la Banque une demande d'exemption similaire dès que leur interface dédiée respectera les exigences légales en la matière. Compte tenu de la complexité et de la multitude des produits de paiement offerts par les banques, la mise au point de l'interface dédiée requiert plus de temps qu'initialement prévu.

S'agissant de l'application d'une authentification forte des clients[1] pour l'initiation et l'exécution sécurisées des paiements (tant les paiements par carte que les virements), l'EBA a publié en juin 2019 un avis qui expose plus en détail quels éléments peuvent être utilisés pour l'authentification forte des clients. Toutefois, il s'est avéré que l'industrie des cartes avait besoin d'un régime transitoire en matière d'utilisation de cartes de paiement dans le commerce en ligne (*e-commerce*). Conformément à l'avis de l'EBA en question et à l'instar de toutes les autres autorités de contrôle de l'UE, la Banque a donc publié, le 28 août 2019, une communication dans laquelle elle reconnaît les défis qu'entraîne le respect de l'authentification forte du client pour les émetteurs belges de cartes de paiement et les acquéreurs belges pour ces transactions par carte effectuées dans le cadre du commerce en ligne, ainsi que la nécessité de coopérer avec les parties concernées (prestataires de services de paiement, schémas de carte de paiement, associations de commerçants et de consommateurs, etc.) pour convenir d'un plan de migration raisonnable et acceptable – dès que raisonnablement possible après le 14 septembre 2019 – devant permettre au secteur de mettre en œuvre l'authentification forte du client pour les paiements par carte dans le commerce en ligne. La Banque s'attend à ce que le secteur établisse un plan de migration, qu'elle devra approuver dans la première partie de 2020 et qui permettra de procéder à cette migration au plus tard le 31 décembre 2020.

L'ouverture de l'infrastructure des comptes de paiement s'accompagne d'exigences de sécurité strictes

2. *Stablecoins* mondiaux

L'une des tendances les plus marquantes de 2019 a été l'émergence des *global stablecoins*, soutenus par des consortiums internationaux. Les initiatives en matière de *global stablecoins* visent à mettre en place une infrastructure financière internationale caractérisée par une monnaie virtuelle stable et un large réseau d'utilisateurs. La stabilité des prix serait créée par le rattachement de la monnaie virtuelle à des avoirs à valeur constante comme les dépôts et les obligations d'État à court terme. En outre, dans les consortiums internationaux souhaitant lancer ces *global stablecoins*, les partenaires possèdent généralement un large réseau d'utilisateurs (par exemple, Facebook en tant que partenaire de Libra) qui doivent soutenir l'utilisation du *stablecoin* comme moyen de paiement. La stabilité des prix et la taille du réseau constituent les défis typiques de la première génération de cryptomonnaies comme Bitcoin.

Par ailleurs, les *stablecoins* mondiaux font apparaitre des défis importants pour le système financier actuel. À l'heure actuelle, le traitement des paiements internationaux est encore souvent inefficace et opaque. De plus, certaines parties du monde se caractérisent par une faible inclusion financière.

Toutefois, l'introduction de *global stablecoins* peut également comporter des risques majeurs. La Banque examine avec d'autres autorités internationales de quels risques il s'agit, par exemple l'utilisation de global stablecoins à des fins de blanchiment de capitaux, de financement du terrorisme ou d'évasion fiscale, ou d'atteintes au respect de la vie privée, à la concurrence et à la protection des consommateurs (notamment la remboursabilité). En outre, il peut y avoir d'importantes implications pour la stabilité financière si le consortium privé ou l'un de ses partenaires perd la confiance du public.

1 L'authentification forte des clients requiert l'utilisation d'au moins deux des trois éléments suivants qui doivent être indépendants et confidentiels : un élément que seul l'utilisateur connaît (par exemple, un code PIN), un élément que seul l'utilisateur possède (par exemple, une carte de paiement) et un élément propre à l'utilisateur (par exemple, des données biométriques, comme une empreinte digitale).

Il convient également de vérifier si l'efficacité d'importants instruments macroéconomiques comme la politique monétaire des banques centrales pourrait être altérée par une percée des *stablecoins*.

La Banque examine avec d'autres autorités internationales quels risques les global stablecoins peuvent comporter

Au moment de la rédaction du présent rapport, il n'a pas pu être établi dans quelle mesure le cadre réglementaire et prudentiel existant était suffisant. Par la coopération internationale, les autorités tentent d'obtenir des informations détaillées sur la conception technique, opérationnelle et organisationnelle des *global stablecoins*. Grâce à une approche coordonnée au niveau international, les autorités s'efforcent d'éviter tout arbitrage réglementaire.

La Banque participe activement à l'amélioration continue des systèmes de paiement exploités par les banques centrales et contribue activement à des analyses y afférentes dans des groupes de travail internationaux, par exemple le Committee on Payments and Market Infrastructures (CPMI).

3. Cyber-risques et risques informatiques

3.1 Poursuite de l'augmentation des cybermenaces et des menaces liées à l'informatique

Dans le monde entier, les cyberattaques sont devenues au cours de ces dernières années une réalité quotidienne. En même temps, l'on observe que certains attaquants affinent les techniques et les méthodes utilisées, rendant certaines des attaques constatées de plus en plus sophistiquées et puissantes. Le nombre de cyberattaques ciblées et de longue durée devrait dès lors encore augmenter à l'avenir, le secteur financier restant logiquement l'une des cibles potentielles. La capacité des cybercriminels à dissimuler parfois l'attaque sur de longues périodes permet le détournement, la diffusion intentionnelle, la modification ou la destruction de données financières sensibles ou critiques. Dans ces circonstances, les établissements financiers et les infrastructures financières font face au défi de protéger adéquatement leurs systèmes, données et services informatiques contre les différentes attaques.

Outre les cyber-risques, la forte dépendance à l'égard des solutions informatiques dans le secteur financier présente également d'autres défis. Les établissements traditionnels sont incités, sous la pression d'acteurs innovants, des attentes croissantes des clients quant aux services offerts et à leur disponibilité, ou de l'augmentation des risques de sécurité (par exemple par l'utilisation de logiciels obsolètes dont le support n'est plus assuré), à renouveler leurs architectures informatiques parfois fort vieillissantes à court terme. En raison de la complexité de leur environnement informatique, c'est un véritable défi de réaliser cet objectif selon des modalités bien contrôlées. Il existe également un risque important de dépendance croissante à l'égard de tiers pour les services informatiques et d'autres composants de systèmes informatiques standardisés. En particulier, les solutions de cloud sont de plus en plus utilisées pour des processus de plus en plus importants. Cette évolution contribue également à ce qu'à l'échelle sectorielle, un nombre limité de prestataires de services critiques présente un risque

de concentration toujours croissant pour le secteur financier. La nécessité de soumettre les solutions de reprise à des tests suffisamment représentatifs reste également un point d'attention important.

L'évaluation et la promotion de la maîtrise des cyber-risques et des risques informatiques constituent dès lors des priorités absolues pour le contrôle prudentiel et l'*oversight* des établissements financiers et des IMF, la coopération européenne et internationale y prenant une importance croissante. Au niveau des établissements individuels, il est vivement recommandé de renforcer encore les mesures et les efforts de protection contre les risques informatiques et les cyber-risques. L'attention nécessaire est accordée par ailleurs aux stratégies de maîtrise sectorielles en cours d'élaboration en Belgique et à l'étranger. Ces deux aspects sont exposés plus en détail dans les paragraphes qui suivent.

3.2 Lignes directrices

Au cours des dernières années, la Banque a contribué dans une large mesure à un cadre réglementaire visant à améliorer la maîtrise des cyber-risques et des risques informatiques. La circulaire prudentielle[1] relative aux attentes de la Banque en matière de continuité et de sécurité opérationnelles des établissements financiers d'importance systémique demeure une référence importante. En outre, la Banque contribue activement à la mise en place d'un cadre réglementaire européen pour la gestion des cyber-risques et des risques informatiques sous les auspices de l'EBA. Cela a conduit par exemple à la publication des orientations de l'EBA à l'intention des autorités de contrôle sur l'évaluation du risque lié aux TIC dans le cadre du SREP pour les établissements de crédit et les entreprises d'investissement[2]. En 2019, cela a mené, d'une part, à des orientations sur l'externalisation[3], qui ont depuis été intégrées dans les politiques de la Banque, et, d'autre part, à des orientations sur la gestion des risques liés aux TIC et à la sécurité[4]. Pour les entreprises d'assurance, la Banque contribue également à la mise en place d'un cadre réglementaire similaire sous l'égide de l'EIOPA.

Dans le monde entier, les cyberattaques sont devenues au cours de ces dernières années une réalité quotidienne

En ce qui concerne les IMF, le CPMI a réuni en décembre 2019 des experts du secteur afin de continuer à concrétiser sa stratégie visant à réduire le risque de fraude dans les paiements de gros. Cela a conduit au recensement et à la formalisation de nouvelles mesures dont l'efficacité a été prouvée. En sa qualité de coprésidente de ce groupe de travail au sein du CPMI, la Banque y a apporté une contribution significative. La Banque, à l'instar des autres banques centrales membres de ce groupe de travail, travaille également à la mise en œuvre de cette stratégie.

3.3 Activités opérationnelles

Les cyber-risques et les risques informatiques constituent un point d'attention pour la Banque dans le cadre de son contrôle prudentiel et de son *oversight*. Dans ce domaine, elle s'intéresse, d'une part, à la protection des établissements financiers ou IMF individuels et à la confiance qu'ils inspirent, et, d'autre part, au secteur dans son ensemble.

L'approche pour les établissements individuels est double. D'une part, les établissements soumis au contrôle prudentiel doivent détenir des fonds propres pour couvrir leurs risques opérationnels, qui comprennent les cyber-risques et les risques informatiques. D'autre part, la sécurité opérationnelle et la robustesse des processus critiques des établissements financiers et des IMF font l'objet d'un suivi attentif. La disponibilité, l'intégrité et la confidentialité des systèmes informatiques et des données sont à cet égard essentielles. La Banque a effectué plusieurs missions d'inspection en 2019 (pour les banques, dans le cadre du SSM) afin de vérifier le respect du cadre réglementaire et la gestion adéquate des systèmes informatiques en matière de cyber-risques et de risques informatiques. Par ailleurs, la Banque procède au suivi de ces risques auprès des établissements financiers et des IMF dans le cadre de ses activités de contrôle permanentes et récurrentes.

1 Circulaire NBB_2015_32 du 18 décembre 2015 relative aux attentes prudentielles complémentaires en matière de continuité et de sécurité opérationnelles des établissements financiers d'importance systémique.

2 Orientations de l'EBA sur l'évaluation du risque lié aux TIC dans le cadre du processus de contrôle et d'évaluation prudentiels (SREP), mai 2017.

3 Orientations de l'EBA relatives à l'externalisation, février 2019.

4 EBA Guidelines on ICT and security risk management (novembre 2019 – traduction française à paraître).

La Banque accorde également une attention croissante aux initiatives sectorielles. Ainsi, le SSM effectue régulièrement des analyses transversales sur des sujets liés à l'informatique et aux aspects cybernétiques. Il a par exemple été demandé en 2019 à toutes les banques importantes ainsi qu'à certaines banques moins importantes de répondre à un questionnaire qui doit fournir, pour les aspects informatiques, des renseignements importants pour le SREP annuel, et qui permettra par ailleurs de procéder à des analyses transversales. Il a également été demandé à une série d'entreprises d'assurance de fournir des renseignements similaires à des fins comparables.

Dans son rôle d'autorité sectorielle pour l'application de la loi relative à la sécurité et la protection des infrastructures critiques (principalement les banques et IMF d'importance systémique), la Banque évalue également l'efficacité des systèmes de contrôle de ces infrastructures financières critiques. C'est également dans ce cadre que la Banque organise et coordonne des exercices sectoriels de simulation de crise, afin de préparer le secteur financier belge à d'éventuels incidents opérationnels de nature systémique. Dans le cadre de la loi pour la sécurité des réseaux et des systèmes d'information, la Banque fait office de point de contact sectoriel pour les incidents survenant dans le secteur financier.

Enfin, depuis le second semestre 2018, la Banque a mis en place un cadre pour le piratage éthique, baptisé TIBER-BE (*Threat Intelligence-Based Ethical Red Teaming Belgium*). Ce programme constitue le volet belge d'une méthodologie qui a été élaborée par l'Eurosystème et vise, au moyen de tests sophistiqués, à accroître la cyberrésistance des établissements financiers et des IMF individuels ainsi qu'à fournir des observations importantes sur la cybersécurité du secteur financier belge dans son ensemble. La Banque encourage ces exercices en sa qualité de gardienne de la stabilité financière ; ces tests s'opèrent dès lors indépendamment de ses responsabilités en matière de contrôle prudentiel et d'*oversight*. TIBER-BE a continué à être mis en œuvre au cours de l'année sous revue.