N° 607

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

QUINZIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale le 31 janvier 2018

RAPPORT

FAIT

AU NOM DE LA COMMISSION DES FINANCES, DE L'ÉCONOMIE GÉNÉRALE ET DU CONTRÔLE BUDGÉTAIRE SUR LE PROJET DE LOI, après engagement de la procédure accélérée, *ratifiant l'ordonnance n° 2017-1252 du 9 août 2017 portant transposition de la directive 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les* **services** *de* **paiement** *dans le* **marché intérieur** (n° 368)

PAR MME NADIA HAI

Députée

SOMMAIRE

INTRODUCTION

À l'image de nombreux secteurs, l'accélération de la transformation des services de paiement est marquante depuis quelques années. Elle résulte, bien entendu, de l'innovation dans le domaine des nouvelles technologies et de leur diffusion. L'effet de ces dernières est double : d'une part, elles bouleversent les modalités d'exercice des activités traditionnelles du secteur ; d'autre part, elles engendrent de nouvelles activités de services de paiement, exercées par des prestataires tiers.

Par ces deux dynamiques, elles favorisent l'amélioration de la qualité de service pour le consommateur. Celui-ci dispose d'abord d'un meilleur accès à l'information, qui lui permet non seulement de s'impliquer davantage personnellement dans la gestion de son patrimoine financier, mais également de comparer plus aisément les offres des différents prestataires de services de paiement (PSP), en particulier des établissements de crédit. Une grande partie de l'amélioration de la diversité et de la qualité des services qui lui sont rendus s'explique par la possibilité de traiter ces données et de les analyser.

Les opportunités qui s'offrent à l'utilisateur des services de paiement par le traitement et l'accès à certaines données ont pour contrepartie l'émergence de risques quant à la protection de la vie privée et à la sécurité des données. Ces risques communs à l'ensemble des services de paiement sont d'une ampleur d'autant plus grande que la circulation des données est facilitée.

Pour que le consommateur et l'ensemble de l'économie tirent parti de ces évolutions, le droit dérivé européen s'est attaché à créer les conditions de la construction d'un marché intérieur dans le secteur des services de paiement. Il s'est agi d'encourager l'innovation et la concurrence au sein du marché européen. À cet effet, la directive 2007/64/CE concernant les services de paiement dans le marché intérieur [(1)], dite « DSP1 », a posé les premiers jalons en mettant fin au monopole bancaire dans les services de paiement.

Compte tenu des évolutions rapides du secteur, il était nécessaire que l'Union actualise ces normes en régulant les activités apparues depuis l'adoption de DSP 1. La directive 2015/2366 du 2015/2366 concernant les services de paiement dans le marché intérieur [(2)], dite « DSP 2 », a donc renouvelé le cadre juridique européen applicable à ces services. Elle confère un statut juridique à deux types d'acteurs : les prestataires de services d'initiation de paiement (PSIP) et les prestataires de services d'information sur les comptes (PSIC).

---

(1) Directive 2007/64/CE du Parlement européen et du Conseil du 13 novembre 2007 concernant les services de paiement dans le marché intérieur, modifiant les directives 97/7/CE, 2002/65/CE, 2005/60/CE ainsi que 2006/48/CE et abrogeant la directive 97/5/CE.

(2) 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.

L'article 115 de DSP 2 avait fixé la date avant laquelle les États membres devaient transposer la directive au **13 janvier 2018**, date de l'entrée en vigueur de la plupart de ses dispositions. À cette fin, le législateur, par l'article 70 de la loi du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique [(1)], dite « loi Sapin 2 », avait habilité le Gouvernement à prendre par ordonnance les mesures requises. Sur ce fondement, l'ordonnance du 9 août 2017 portant transposition de la directive 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur [(2)] a modifié le code monétaire et financier, afin de transposer ces dispositions dans le droit interne.

La directive n'est toutefois pas entièrement applicable, l'entrée en vigueur de certains de ses articles (articles 65, 66, 67 et 97) étant prévue dans un délai de dix-huit mois suivant la publication de **normes techniques de réglementation (NTR)** qui doivent faire l'objet d'un règlement délégué de la Commission. Celle-ci a présenté son projet de règlement délégué le 27 novembre 2017. Le Parlement européen et le Conseil de l'Union européenne ont par conséquent jusqu'au 27 février 2018 pour les examiner. En l'absence d'examen, elles seront adoptées et l'ensemble des dispositions de la directive sera applicable à la fin du mois d'**août 2019**. Jusqu'à cette date, les règles actuelles continuent de s'appliquer. Cette période de transition concerne en particulier les modalités d'accès des PSIP et des PSIC à certaines données des comptes de paiement, l'obligation d'identification de ces derniers auprès des gestionnaires des comptes pour accéder aux données nécessaires à leur activité et le renforcement des exigences d'authentification pour l'accès au compte et les opérations à distance.

Le présent projet de loi vise à ratifier l'ordonnance du 9 août 2017 précitée. Il procède également à des corrections d'erreurs ou de coordinations à la suite de l'entrée en vigueur de l'ordonnance.

(1) Loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique.

(2) Ordonnance n° 2017-1252 du 9 août 2017 portant transposition de la directive 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur.

EXPOSÉ GÉNÉRAL

La directive DSP 2 s'inscrit dans la lignée de DSP 1 qu'elle abroge. Elle adapte le cadre juridique européen de ces services aux évolutions du secteur et poursuit l'objectif général de réalisation du marché intérieur. Comme indiqué *supra*, l'article 70 de la loi « Sapin 2 » a habilité le Gouvernement à prendre par ordonnance les mesures relevant du domaine de la loi nécessaires à la transposition de DSP 2.

Il a également habilité le Gouvernement à prendre par ordonnance les mesures d'ordre législatif permettant de :

– rendre applicables en Nouvelle-Calédonie, en Polynésie française et à Wallis-et-Futuna les articles du code monétaire et financier et, le cas échéant, d'autres codes et lois, dans leur rédaction résultant de la transposition de la directive précitée, avec les adaptations nécessaires pour celles qui relèvent de la compétence de l'État ;

– procéder aux adaptations nécessaires de ces articles concernant les collectivités de Saint-Barthélemy, de Saint-Martin et de Saint-Pierre-et-Miquelon.

I. LA NÉCESSITÉ DE RENOUVELER LE CADRE JURIDIQUE EUROPÉEN

● La directive DSP 1 avait harmonisé les règles applicables aux services de paiement dans les États membres, afin d'assurer la coordination de dispositions nationales alors fragmentées, de garantir l'accès au marché de nouveaux prestataires de services de paiement, de fixer des exigences d'informations et de définir les droits et obligations des utilisateurs et prestataires de services de paiement.

Pour stimuler la concurrence sur le marché des services de paiement, elle avait instauré un **agrément unique** pour tous les prestataires de services de paiement étrangers à l'activité de réception des dépôts ou d'émission de monnaie électronique. À cette fin, elle a créé la catégorie juridique des **établissements de paiement**, mettant par là un terme au monopole des établissements bancaires en la matière.

Les innovations du secteur ont rendu nécessaire une rénovation du corpus des normes européennes le régissant. Comme il est indiqué dans les considérants de la directive DSP 2, l'apparition de nouveaux types de services de paiement et la croissance rapide des paiements électroniques et mobiles ont mis à l'épreuve le système de règles alors en vigueur.

● Il s'est agi de répondre aux questions juridiques soulevées par le développement de certains acteurs du monde de la *Fintech*. Les **activités des services d'initiation de paiement (SIP)** ou des **services d'information sur les comptes (SIC)**, nécessitent en effet un accès à certaines données des utilisateurs de services de paiement, ce qui implique l'existence de canaux d'identification. À l'heure actuelle, alors que la directive DSP 2 n'est pas entièrement entrée en vigueur, la plupart des PSIC accèdent aux comptes bancaires en ligne de leurs clients en se faisant passer pour eux, méthode dite du « *web scraping non identifié* », du « *screen scraping non identifié* » ou de « l'accès direct non identifié ». Elle présente des fragilités juridiques, en particulier s'agissant du régime de responsabilité.

Le *web scraping*, *screen scraping* ou « accès direct »

Le *web scraping* est une méthode d'extraction de données dont l'origine remonte à une quinzaine d'années. Elle consiste à extraire d'une page internet des informations spécifiquement recherchées. Elle est notamment utilisée par les moteurs de recherche et leur permet de détecter des mots-clefs dans les pages web afin de proposer celles d'entre elles qui sont les plus pertinentes.

Cette méthode est également utilisée par de nombreux prestataires de services de paiement. Les PSIC et les PSIP en usent pour obtenir, avec leur consentement, les données bancaires de leurs clients détenues par les établissements gestionnaires de compte. Actuellement, ces prestataires tiers accèdent aux données en se faisant passer pour l'utilisateur du compte *via* l'interface que les banques mettent à la disposition de leurs clients. Pour ce faire, ils utilisent les identifiants et mots de passe de ces derniers.

Le *web scraping* non identifié est risqué en ce qu'il favorise la circulation des identifiants et des données bancaires. Il ne permet pas non plus un partage optimal des responsabilités en cas d'opérations frauduleuses, compte tenu du défaut d'identification.

Il y a lieu de distinguer la technique d'accès elle-même des modalités d'usage de cette technique, qui peuvent comporter un risque par le stockage de certaines données et l'absence d'identification des prestataires tiers lorsqu'ils accèdent aux données.

● Enfin, les marchés des paiements par carte, par internet et par téléphone répondaient à des logiques essentiellement nationales. Or, comme pour les autres services de paiement, une plus grande intégration des marchés nationaux a pour avantage d'encourager l'innovation, grâce à une concurrence accrue. Le consommateur bénéficie d'une plus grande diversité de choix et d'une meilleure transparence, d'économies d'échelle et de l'amélioration de la sécurité des paiements [(1)].

(1) Commission européenne, livre vert « Vers un marché européen intégré des paiements par carte, par internet et par téléphone mobile *», 11 janvier 2012.*

II. LES PRINCIPALES ORIENTATIONS DE LA DIRECTIVE 2015/2366 CONCERNANT LES SERVICES DE PAIEMENT DANS LE MARCHÉ INTÉRIEUR

La directive DSP 2 a donc apporté plusieurs modifications substantielles au droit antérieurement applicable aux services de paiement.

● Elle dessine un cadre juridique aux activités de deux nouvelles catégories d'acteurs évoqués précédemment :

– les **prestataires de services d'initiation de paiement (PSIP)**, dont l'activité consiste à **initier un ordre de paiement à la demande de l'utilisateur des services de paiement** concernant un compte de paiement détenu auprès d'un autre prestataire de services de paiement. Ils permettent aux consommateurs de payer leurs achats en ligne par simple virement, tout en donnant aux commerçants l'assurance que le paiement a été initié, de sorte que les biens peuvent être livrés ou les services fournis sans délai. Ces services demeurent peu développés en France, mais leur utilisation est plus fréquente dans d'autres États membres, comme en Allemagne ou aux Pays-Bas. L'entreprise allemande Sofort et l'entreprise hollandaise iDeal font par exemple partie des leaders du secteur en Europe. Aujourd'hui, le marché des SIP représente environ 2,5 millions d'utilisateurs en France et plus de 50 millions en Europe ;

– les **prestataires de services d'information sur les comptes (PSIC)** que l'on appelle également agrégateurs d'informations, dont l'activité consiste en la fourniture d'informations consolidées concernant un ou plusieurs comptes de paiement détenus par un utilisateur de services de paiement auprès d'un ou plusieurs prestataires de services de paiement. Le client de ces services a donc une vision consolidée de ses comptes sur une seule interface, indépendante des banques gestionnaires de ces différents comptes. Plusieurs acteurs ont trouvé un marché en France, comme les entreprises Bankin, qui revendique plus de 2 millions d'utilisateurs en Europe, Linxo (1,6 million d'utilisateurs), ou Budget Insight, qui proposent leurs services directement ou par l'intermédiaire de tiers. Au total, le marché des SIC représente 4 millions d'utilisateurs en France (dont 200 000 entreprises) et 15 millions en Europe.

La directive encadre ces activités en prévoyant des **exigences d'agrément et d'enregistrement**, respectivement pour les PSIP et les PSIC, compte tenu des différences de nature entre ces activités (articles 11.1 et 33.1 de la directive).

Il faut noter que ces deux types de prestataires ne détiennent pas les fonds des clients. C'est la raison pour laquelle le législateur européen a décidé de leur appliquer des **règles en fonds propres dérogatoires** (article 9.1). Néanmoins, la directive leur impose de disposer d'une **assurance de responsabilité civile professionnelle** couvrant les territoires où ils proposent des services ou une autre garantie comparable (article 5.2). Conformément à l'article 5.4, l'Autorité bancaire européenne (ABE) a émis des orientations concernant les critères que les États

membres doivent utiliser pour fixer le montant minimal de l'assurance de responsabilité civile [(1)].

En créant un statut juridique à ces acteurs, la directive garantit en même temps le droit aux utilisateurs de recourir à des PSIP ou à des PSIC en imposant aux gestionnaires des comptes de paiement (généralement les banques) des obligations de communication d'informations à ces nouveaux acteurs (articles 66 et 67). Elles font partie des dispositions qui devraient entrer en vigueur, dans le droit européen, dix-huit mois après la publication du règlement dérivé de la Commission concernant les normes techniques de réglementation (NTR).

● Sans les bouleverser, la directive modifie les **règles générales applicables aux établissements de paiement**. Les conditions de délivrance des agréments sont notamment complétées (article 5).

● La directive DSP 2 renforce les **normes de sécurité des données** concernant l'accès du client à son compte de paiement en ligne, les opérations de paiement électronique et l'exécution de toute action effectuée à distance comportant un risque de fraude en matière de paiement ou de toute autre utilisation frauduleuse. Dans ces trois situations, elle exige un **système d'authentification forte** (article 97), c'est-à-dire un système qui combine plusieurs facteurs d'authentification. Les caractéristiques de ce système seront également précisées par les NTR.

● Plusieurs dispositions renforcent les **droits des utilisateurs de services de paiement**. En cas d'opération de paiement non autorisée, la directive impose au prestataire de services de paiement du payeur de lui rembourser le montant de l'opération immédiatement après avoir pris connaissance de l'opération et, au plus tard, à la fin du premier jour ouvrable suivant, cette obligation ne s'appliquant pas dans le cas où le prestataire de services de paiement soupçonne le payeur de fraude, auquel cas il est tenu d'en informer l'autorité nationale concernée (article 73). Dans le cas d'une utilisation frauduleuse d'un instrument de paiement consécutivement à une perte ou un vol, il reste possible au prestataire de laisser à la charge de l'utilisateur une part des pertes occasionnées, dans la limite d'un montant plafond. La directive DSP 2 a toutefois abaissé ce plafond de **150 à 50 euros** (article 74).

Elle prévoit, dans la même veine, que les services de paiement mettent en place une **procédure de réclamation** que les utilisateurs de services de paiement peuvent suivre avant l'engagement d'une procédure de règlement extrajudiciaire ou judiciaire (article 99). Le **régime de contestation et de remboursement des opérations de paiement** est rendu plus favorable au payeur, qu'il s'agisse d'opérations de paiement non autorisées (article 74), d'opérations de paiement dont le montant n'est pas connu à l'avance (article 75) ou d'opérations de paiement initiées par le bénéficiaire (articles 76 et 77).

---

(1) Orientation sur l'assurance de responsabilité professionnelle au titre de la directive DSP 2, *Autorité bancaire européenne, 12 septembre 2017.*

● La directive renforce la **supervision transfrontalière des établissements de paiement**.

Elle instaure un système de règlement des différends entre les autorités de supervision des États membres sur les questions de coopération transfrontalière, en prévoyant la possibilité pour ces autorités de demander l'assistance de l'ABE (article 27).

Elle installe une procédure d'échanges d'informations entre les autorités de supervision permettant de faciliter l'exercice du droit d'établissement et de la liberté d'installation des établissements de paiement (article 28).

Elle renforce les échanges entre les autorités compétentes dans le cadre de la surveillance des établissements de paiement et laisse la possibilité aux États membres d'exiger des établissements de paiement exerçant sur leur territoire en vertu du droit d'établissement qu'ils désignent un point de contact central sur leur territoire (article 29).

Elle étend les pouvoirs des États membres d'accueil en cas de non-conformité des établissements de paiement aux règles générales s'imposant à eux (article 30).

III. L'APPLICATION DES PRINCIPES DE LA DIRECTIVE ET LES PERSPECTIVES D'EXTENSION DE CERTAINES RÈGLES

Bien que la plupart des dispositions de la directive soient applicables depuis le 13 janvier 2018, la finalisation des NTR et leur traduction opérationnelle constituent un enjeu majeur, à la fois pour les acteurs traditionnels et pour les acteurs plus récents. Il en va de même s'agissant de l'hypothèse d'un élargissement des règles de la directive aux comptes autres que les comptes de paiement. Enfin, la directive permet aux États membres de laisser la possibilité aux commerçants de fournir des espèces à leurs clients.

A. L'ADOPTION DES NORMES TECHNIQUES DE RÉGLEMENTATION ET LA PÉRIODE TRANSITOIRE AVANT LEUR ENTRÉE EN VIGUEUR

La directive DSP 2 impose aux gestionnaires de compte de communiquer de manière sécurisée aux prestataires de services tiers les informations nécessaires à l'exercice de leur activité. Ils devront également traiter les demandes d'initiation des SPIP et les demandes de données des SPIC de manière non discriminatoire.

De leur côté, les SPIP et les SPIC devront alors satisfaire à des exigences de sécurité des données et seront dans l'obligation de s'identifier auprès du gestionnaire lorsqu'ils souhaitent accéder aux données bancaires.

Ces dispositions, comme les dispositions relatives à l'authentification forte, **n'entreront en vigueur qu'à l'issue de la période de transition de dix-huit mois suivant la publication du règlement délégué de la Commission européenne relatif aux normes techniques de réglementation**. La proposition de la Commission a été publiée le 27 novembre 2017. Elle devrait être adoptée à la fin du mois de février 2018. En conséquence, l'ensemble de ces dispositions seront applicables en **août 2019**.

Cette proposition de règlement prévoit que l'accès direct de tiers sans identification (*web scraping* ou *screen scraping*), ne sera plus autorisé. Néanmoins, à l'issue de cette période, il reviendra aux gestionnaires de compte de développer et de maintenir une **interface de communication ouverte et sécurisée** permettant aux services de paiement tiers d'accéder aux données dont ils ont besoin. Jusqu'à l'application de ces dispositions, ce sont les règles d'accès actuelles qui prévalent. Le *web scraping* non identifié demeure donc autorisé.

En France, les principaux établissements bancaires promeuvent un modèle d'interfaces standardisées, ouvertes et sécurisées dites « API » pour *Application Programming Interface*.

Pour s'assurer de l'efficacité de l'interface, l'article 30 du projet de règlement prévoit deux garanties. D'une part, les spécifications techniques des interfaces devront faire l'objet d'une **documentation précise**, qui sera mise à disposition des PSIP, des PSIC ou des prestataires de services de paiement qui émettent des instruments de paiement liés à une carte, au moins six mois avant la fin de la période de transition, dès lors que ces derniers ont été agréés par les autorités nationales. D'autre part, les gestionnaires doivent également leur mettre à disposition un **dispositif d'essai** permettant des tests de connexion et de fonctionnement au moins six mois avant l'application des normes.

En cas de performance insuffisante des interfaces ou d'absence de ces interfaces, le projet de règlement de la Commission (article 33) prévoit un **mécanisme de secours** qui prendrait la forme d'un **accès direct et identifié** des prestataires de paiement tiers aux données par l'ouverture par les gestionnaires des interfaces utilisateur. Néanmoins, les États membres peuvent exempter les banques de cette obligation d'ouverture si les conditions suivantes sont remplies [(1)] : l'interface satisfait aux obligations prévues par les normes NTR ; elle a été testée par les PSIP et par les PSIC agréés qui l'ont demandé ; elle a été largement utilisée pendant au moins trois mois ; tout problème lié à l'interface dédiée a été résolu sans retard injustifié.

Si les établissements de crédit ne prévoient pas de permettre aux PSIP et aux PSIC un accès identifié aux données bancaires par leur interface client, au titre du mécanisme de secours, il conviendra de s'assurer que les conditions présentées ci-dessus sont rigoureusement respectées.

(1) Exposé des motifs du projet de règlement délégué de la Commission complétant la directive 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.

La date à partir de laquelle courra la période de transition a été, dans les faits, retardée par rapport à celle que l'on aurait raisonnablement pu attendre au moment de la publication de DSP 2. Cette différence a pour cause la longueur inattendue de l'édiction des propositions de NTR, qui ont fait l'objet de divergences entre l'ABE et la Commission.

Durant cette période, les modalités d'accès aux données bancaires ne présentent pas des niveaux de sécurité satisfaisants. La rapporteure soutiendra donc toute proposition du Gouvernement qui viserait à accélérer l'entrée en vigueur de l'accès par interfaces sécurisées, dès lors que l'ensemble des garanties de performance des interfaces entrent en vigueur concomitamment.

B. LA SITUATION DES COMPTES AUTRES QUE LES COMPTES DE PAIEMENT

Aux termes de son article 3, la directive DSP 2 ne couvre pas les opérations liées à des comptes autres que les comptes de paiement. Les comptes d'épargne et les comptes d'assurance, par exemple, n'entrent pas dans son champ.

Or, le problème des modalités d'accès aux données financières des SPIP et des SPIC se pose dans les mêmes termes s'agissant de l'accès à ces comptes, d'autant plus que la plupart des comptes qu'agrègent les SPIC ne sont pas des comptes de paiement. La démarche consistant à élargir les nouvelles normes de régulation à ces comptes n'est pas dénuée de tout fondement, ne serait-ce que par l'incertitude que la situation actuelle fait prévaloir s'agissant des régimes de responsabilité. En l'état, les obligations de mise à disposition par les banques d'une interface d'échanges de données ne s'appliqueraient que pour les comptes de paiement, l'accès aux autres comptes devant alors se faire selon les mêmes modalités qu'actuellement.

Néanmoins, à court terme, il ne serait pas opportun de s'engager dans la voie de l'élargissement des règles que l'ordonnance transpose aux autres comptes. Alors que le Gouvernement évalue les mesures de transposition du droit européen qui vont au-delà de ce qui est nécessaire à son application [(1)], il ne serait pas de bonne méthode d'étendre le champ de la directive dans le projet de loi de ratification de l'ordonnance de transposition, sans une évaluation précise des impacts d'une telle extension. En tout état de cause, la rapporteure estime que le sujet doit être traité au niveau européen, ce qui requiert la consultation de l'ensemble des parties prenantes. À ce stade, ces discussions n'ont pas débuté.

Une réflexion devra toutefois s'engager sur le sujet.

(1) Circulaire du 26 juillet 2017 relative à la maîtrise du flux des textes réglementaires et de leur impact.

C. L'OUVERTURE AUX COMMERÇANTS DE LA POSSIBILITÉ DE RENDRE LA MONNAIE EN ESPÈCES OU « CASHBACK »

La directive DSP 1 excluait déjà de son champ d'application « *les services pour lesquels des espèces sont fournies par le bénéficiaire au bénéfice du payeur dans le cadre d'une opération de paiement, à la demande expresse de l'utilisateur de services de paiement formulée juste avant l'exécution de paiement via un paiement pour l'achat de biens ou de services* », aux termes du e) de son article 3. Il s'agit de l'activité permettant à un particulier de se rendre dans un commerce pour solliciter, lors d'un achat, la mise à disposition d'espèces en contrepartie d'un paiement par carte correspondant au prix du bien acheté augmenté du montant des espèces ainsi obtenues. Elle est souvent appelée « ***cashback*** ». L'exclusion de la directive signifie qu'il n'est pas nécessaire d'être un prestataire de services de paiement pour proposer ce type de services.

En l'absence de dispositions de transposition, le *cashback* est applicable en France depuis l'entrée en vigueur de la directive DSP 1, sans plus de précision quant à ses modalités d'application. Il est donc déjà possible pour un commerçant, en théorie, de rendre la monnaie en espèces à l'occasion d'une transaction d'un bien ou d'un service effectuée par carte bancaire. Le droit applicable était toutefois trop incertain pour que les commerçants réalisent les investissements nécessaires à sa mise en œuvre.

La directive DSP 2 reprend la même exclusion. Plusieurs arguments plaident pour l'édiction de règles plus précises sur les conditions d'exercice de cette activité. Sans encadrement, le développement de la pratique pourrait être porteur de risques liés à la circulation de faux billets ou au blanchiment.

Rappelons qu'en outre, le *cashback* est répandu dans plusieurs pays européens, comme l'Italie, l'Allemagne, le Royaume-Uni et l'Espagne. Les enseignements du fonctionnement de ce système à l'étranger plaident pour qu'il se développe en France. Ses avantages sont connus :

– il améliore l'efficacité des paiements pour le consommateur en réduisant le nombre d'opérations ;

– il diversifie le choix pour le consommateur en lui offrant de nouvelles options pour retirer des espèces, fonction essentielle dans certaines zones souffrant d'un maillage lâche de distributeurs de billets ;

– il offre de nouvelles opportunités pour les commerçants, en attirant des consommateurs, par exemple.

Les représentants des commerçants avec lesquels la rapporteure a pu échanger sont favorables à ce que l'on octroie la possibilité à ces derniers de proposer ce service. Dans l'hypothèse où cette possibilité serait ouverte, il conviendra de fixer un montant plafond de retrait, afin de limiter le risque de blanchiment et d'assurer la probité du circuit fiduciaire. La Banque de France devrait pouvoir restreindre ou élargir ce service en cas d'augmentation anormale de faux billets en circulation.

La rapporteure soutiendra toute initiative du Gouvernement en ce sens.

EXAMEN EN COMMISSION

La commission examine le présent projet de loi au cours de sa séance du 31 janvier 2018.

Mme Nadia Hai, rapporteure. Comme de nombreux secteurs, les activités de services de paiement en Europe ont été profondément transformées par l'innovation technologique. Il en a résulté un manque d'harmonisation des règles applicables à ces services, constituant un frein à la réalisation du marché intérieur, si bien que le consommateur ne peut pas tirer un avantage optimal des innovations et du marché.

Des avancées technologiques ont également conduit à rénover des pratiques anciennes et à en façonner de nouvelles. Elles s'appuient en particulier sur l'accès aux données des utilisateurs et sur leur traitement. Deux types d'acteurs nouveaux sont apparus : d'abord les services d'initiation de paiement, qui donnent des ordres de paiement à la demande d'un utilisateur à partir d'un compte de paiement détenu auprès d'une banque, ensuite les services d'information sur les comptes, qui fournissent des informations consolidées sur les différents comptes d'un utilisateur, qu'ils soient gérés par une ou plusieurs banques.

Actuellement, ces services accèdent aux données des clients des banques grâce aux identifiants de ces derniers. Autrement dit, pour accéder à leurs données bancaires, ils se font passer pour eux, sur le site de leur banque. C'est la technique de l'accès direct non identifié ou *web scraping* non identifié. En l'absence de régulation, l'accès de ces acteurs aux données bancaires fragilise la sécurité des données.

Ces évolutions ont donc rendu indispensable une adaptation du cadre juridique européen. Celle-ci s'est matérialisée par l'adoption de la directive du 23 novembre 2015 sur les services de paiement dans le marché intérieur, dite directive DSP 2. La plupart de ses dispositions sont applicables depuis le 13 janvier 2018. Certaines parmi les plus importantes n'entreront toutefois en vigueur que dans le courant de l'année 2019.

Premièrement, la directive DSP 2 donne un statut juridique aux activités de services d'initiation de paiement et de services d'information sur les comptes. Cette reconnaissance s'accompagne de l'obligation pour les gestionnaires de comptes de paiement – à savoir les banques –, de mettre à disposition les informations nécessaires à l'exercice de leur activité.

Les transmissions de ces données doivent se faire dans un cadre sécurisé, par l'intermédiaire d'une interface ouverte et sécurisée que les banques devront mettre à disposition des initiateurs de paiement et des agrégateurs de données. Ces derniers devront s'identifier *via* cette plateforme et la pratique du *web scraping* non identifié sera interdite.

Pour l'application de cette obligation, la directive renvoie à la Commission européenne le soin de proposer des normes techniques de réglementation (NTR). Ces exigences entreront en vigueur au terme d'une période de transition de dix-huit mois suivant l'adoption de ces normes. En attendant, les initiateurs de paiement et les agrégateurs de compte pourront continuer à utiliser le *web scraping* non identifié pour accéder aux informations bancaires nécessaires à leurs activités.

Outre les modalités d'accès aux comptes, la directive fixe les règles concernant le régime de responsabilité en cas d'opération mal réalisée : elle oblige les initiateurs de paiement et les agrégateurs à disposer d'une assurance civile professionnelle pour couvrir les sommes à rembourser en cas de reconnaissance de leur responsabilité.

Deuxièmement, la directive renforce les exigences de sécurité concernant l'accès du client à son compte de paiement en ligne, en exigeant l'authentification forte. Il s'agit d'une technique de connexion combinant plusieurs facteurs d'identification.

Troisièmement, elle renforce les droits des utilisateurs des services de paiement. Par exemple, elle diminue de 150 à 50 euros la limite du montant que les prestataires de services de paiement peuvent imposer à leur client en cas d'utilisation frauduleuse de leur instrument de paiement.

Enfin, quatrièmement, les règles de supervision et de coopération transfrontalière sont renforcées. Les conditions d'agrément des services de paiement sont complétées. La communication entre les différentes autorités de supervision des États membres, dans le cadre du droit d'établissement et de la liberté de prestation de services, est rendue plus systématique.

L'ordonnance du 9 août 2017 a transposé ces dispositions dans le code monétaire et financier, en vertu de l'habilitation conférée par l'article 70 de la loi « Sapin 2 ». Celle-ci fait l'objet du présent projet de loi de ratification venant en discussion car l'application de la directive et sa transposition dans le droit interne comportent quelques enjeux importants. Je vais en évoquer rapidement trois.

Le premier enjeu concerne l'application des normes NTR que la Commission va proposer et la période de transition avant laquelle elles entreront en vigueur. Après prise en compte de l'avis de l'Autorité bancaire européenne, la Commission a préparé une proposition qui pourrait être adoptée à la fin du mois de février, ce qui déclencherait le début de la période transitoire de dix-huit mois prévue par la directive.

La proposition précise les exigences des interfaces mises à disposition des prestataires de paiement tiers : elles devront être aussi performantes que celles que les banques mettent à disposition de leurs clients. En cas de défaillance de ces interfaces, la proposition de la Commission prévoit un mécanisme de secours pour que les prestataires tiers puissent accéder aux données des banques par leur interface utilisateur, mais en s'identifiant comme prestataires tiers.

Les banques peuvent toutefois être exemptées de cette obligation si certaines conditions garantissant le bon fonctionnement des interfaces dédiées sont respectées. Durant la phase de transition, les interfaces en question seront testées, en particulier par les prestataires tiers.

Les banques françaises ont décidé de développer des interfaces dites *Application programming interface* (API), qui semblent correspondre aux critères de sécurité de la Commission. Pour accéder aux données bancaires, les prestataires tiers auraient donc l'obligation de s'identifier, *via* ces interfaces, à l'issue de la période de transition, c'est-à-dire en août 2019. Or, à l'origine, ces dispositions auraient dû entrer en vigueur bien plus tôt. De longues discussions entre l'Autorité bancaire européenne et la Commission sur les normes NTR expliquent en effet un retard significatif dans d'application de la directive. La période d'incertitude est donc plus longue que prévu. Le Gouvernement pourrait déposer un amendement proposant de réduire la période de transition, qui prendrait fin début 2019. Je le soutiendrai.

Le deuxième enjeu concerne le champ de la directive. Actuellement, celle-ci ne concerne que les comptes de paiement. Or, les prestataires tiers proposent des services qui concernent également d'autres types de comptes, comme les comptes d'épargne. Je comprends la logique sous-jacente à la proposition d'étendre les règles de la directive DSP 2 aux comptes de paiement, mais je crois qu'une telle extension doit s'inscrire dans un cadre européen. Nous y reviendrons lors de l'examen des amendements.

Enfin, le troisième enjeu de la discussion concerne ce que l'on appelle le *cashback*. Il s'agit de la possibilité pour les commerçants de mettre à disposition de leurs clients des espèces en contrepartie d'un paiement par carte correspondant au prix du bien acheté auquel on ajoute le montant des espèces rendues.

Dans les faits, la directive DSP 1, en excluant ce type d'activités de son champ d'application, rendait possible ce service. La directive DSP 2 confirme cette possibilité ; or, en l'absence de dispositions nationales d'application, ledit service ne s'est pas développé. En effet, le cadre juridique étant trop incomplet, les commerçants n'ont pas procédé aux investissements nécessaires. Il serait opportun de poser les premiers jalons pour que cette pratique puisse se développer. Le Gouvernement déposera un second amendement en ce sens.

Pour conclure, la directive DSP 2 comporte un grand nombre de dispositions techniques, mais elle aura, à court et moyen terme, des traductions très concrètes dans la vie de nos concitoyens. J'ai pu le constater lors des auditions que j'ai menées et grâce aux contributions écrites que j'ai reçues depuis une semaine.

Ce projet de loi, tel qu'il sera amendé par le Gouvernement, parvient à atteindre un équilibre entre promotion de l'innovation et protection des données personnelles. Il transpose la directive et rien que la directive.

M. Charles de Courson. Le développement des systèmes du type *bitcoin* est-il visé par la directive ?

Mme la rapporteure. Le *bitcoin* n'est pas concerné par la directive car il ne l'est pas par l'expression « monnaie électronique ».

M. Charles de Courson. Cela signifie-t-il que toutes ces formes de monnaies « privées » peuvent donc continuer de prospérer dans l'indifférence générale ?

Mme la rapporteure. Cela signifie que le *bitcoin* n'est pas concerné par cette directive…

M. Charles de Courson. Il est tout de même assez étonnant de transposer une directive qui a, et à juste raison, pour but de sécuriser les transactions, sans qu'on s'intéresse à la monnaie virtuelle.

M. le président Éric Woerth. Nous transposons une directive et l'idée est de ne pas surtransposer – sur ce point il me semble qu'il y a un accord politique à peu près général. Je rappelle en outre que la commission a précisément créé une mission d'information sur les monnaies virtuelles.

Mme la rapporteure. En effet, une mission d'information va être lancée sur le sujet, vous y êtes le bienvenu, monsieur de Courson.

Mme Amélie de Montchalin. Pour aller dans votre sens, monsieur le président, je rappelle que nous avons décidé, au cours de cette législature, de transposer des directives qui reflètent ce qui a été négocié à vingt-huit ou, prochainement, à vingt-sept. Si des problèmes se posent avec les monnaies virtuelles, en particulier les *bitcoins*, menons un travail législatif comme vous le suggérez afin que nous nous exprimions ensuite d'une voix commune au niveau européen. En effet, surtransposer la directive ne présente ici aucun intérêt car nous savons que les opérations concernées, puisque virtuelles, dépassent le cadre national ; or il faudrait légiférer dans un cadre au minimum européen pour que cela ait du sens. C'est pourquoi, dans un premier temps, examiner cette question dans le cadre de la mission d'information mentionnée m'apparaît tout à fait pertinent.

M. le président Éric Woerth. Donc le *bitcoin* n'est pas concerné par le présent projet de loi, ce qui n'empêche pas que nous examinions ce sujet en profondeur par la suite.

Mme Christine Pires Beaune. Je remercie la rapporteure pour sa présentation très claire et complète. J'ai bien compris que la directive DSP 2 reposait sur deux jambes : le développement innovant des systèmes de paiement d'une part, la protection des données des consommateurs d'autre part. On doit y ajouter la limitation des facturations et franchises acquittées par ces mêmes personnes. Le texte marque par conséquent, en la matière, un progrès incontestable – personne n'en disconviendra, d'autant que le chiffre avancé par la Commission européenne quant au potentiel d'économies que le dispositif permettra de réaliser n'est pas négligeable : 550 millions d'euros.

Néanmoins, ma seule boussole est la protection des consommateurs. Or, l'obligation donnée aux banques de fournir aux prestataires de services de paiement toutes les données et l'accès aux comptes des clients afin d'éviter ce qui se passe actuellement, pourrait néanmoins provoquer des dérives importantes – notamment des fraudes bancaires. Le superviseur, en France, si j'ai bien compris, est l'Autorité de contrôle prudentiel et de résolution (ACPR). Je rappelle que la loi de finances pour 2018 fixe le plafond des autorisations d'emplois pour l'ACPR à 1 050 équivalents temps plein, à savoir une réduction de 7 % du personnel. Aussi je souhaite savoir si la représentation nationale entend accorder les moyens nécessaires à l'ACPR pour exercer ses nouvelles missions.

M. Mohamed Laqhila. J'ai bien compris qu'il ne fallait pas surtransposer cette directive. Toutefois, la protection de l'utilisateur du service de paiement (SP) sera-t-elle la même dans tous les pays de l'Union ? Les transpositions nationales permettront-elles d'adopter des formules différentes. Et, s'il existe des différences de garanties et de protection, quel droit s'appliquera : celui du pays de l'initiateur du paiement ou celui du pays destinataire ?

Mme Véronique Louwagie. Je partage les propos de notre collègue Charles de Courson. Nous ratifions une ordonnance de 2017, transposant une directive de 2015. Cela fait donc trois ans que la directive a été adoptée… J'entends bien que l'on ne peut aborder les sujets relatifs à la monnaie virtuelle dans ce cadre – il ne s'agit pas, vous avez raison, de surtransposer. Mais du fait de ce décalage dans le temps, et de l'évolution technologique, le contenu de la directive n'est-il pas déjà caduc ?

M. le président Éric Woerth. C'est vrai, mais dans ce domaine comme dans d'autres, le régulateur a toujours un peu de retard…

M. Jean-Louis Bourlanges. Ma remarque sera d'ordre méthodologique : je trouve anormal que l'exposé des motifs du projet de loi soit rédigé de la façon dont il nous est présenté. Un exposé des motifs, comme son nom l'indique, doit présenter les motifs d'un projet de loi. Nous devons savoir pourquoi nous votons un texte. Or, ici, on nous dit simplement que cette ordonnance « transpose » et on expose ce dont on parle. On ne nous dit absolument pas à quoi sert ce texte. C'est pourtant le devoir de ceux qui nous le présentent que d'exposer ses objectifs. Sinon on accrédite l'idée que la loi est faite pour traiter de problématiques générales et non pour résoudre des problèmes particuliers. Ma remarque, de portée générale, est parfaitement illustrée par ce texte.

M. Jean Lassalle. Très bien !

M. le président Éric Woerth. Il est vrai que l'exposé des motifs est un peu indigent. Vous avez le soutien de M. Lassalle !

M. Patrick Hetzel. La question se pose effectivement concernant les monnaies virtuelles, mais également au regard des évolutions technologiques elles-mêmes, extrêmement importantes : il est de plus en plus difficile d'assurer la sécurisation des données financières individuelles. Je voudrais abonder dans le sens de mes prédécesseurs : ils ont parfaitement raison, la directive est d'ores et

déjà en retard par rapport à un certain nombre de pratiques. Tous ceux qui s'intéressent à l'intelligence économique savent que les dispositifs de *hacking* sont de plus en plus sophistiqués et que la question de la protection des données personnelles se pose avec une extrême acuité.

Mme la rapporteure. Plusieurs d'entre vous ont soulevé la question de la sécurité des données. Je rappellerai que l'accès aux données est déjà possible *via* le *web scraping* non identifié. L'insécurité juridique existe donc, la protection des données n'étant pas assurée de façon suffisante. La directive concernant les services de paiement dans le marché intérieur permet de sécuriser l'obtention de ces données par le recours à des interfaces opérables, que nous appelons API plus sûres, identifiant la personne qui se connecte.

Monsieur Bourlanges, vous souhaitez connaître l'objet du projet de loi et estimez que l'exposé des motifs n'est pas assez détaillé. Ce projet poursuit trois objectifs : la protection du consommateur, la prise en compte des différents acteurs – banques, initiateurs de paiement et agrégateurs, consommateurs finaux –, et, bien évidemment, la sécurisation des données des consommateurs. Cela figurera dans le rapport.

M. le président Éric Woerth. Le texte du projet de loi – et non votre rapport – est totalement inintelligible pour le commun des mortels.

Mme la rapporteure. Il est extrêmement technique, je vous l'accorde volontiers.

Monsieur Hetzel, madame Louwagie, vous avez évoqué le fait que le délai prévu par la directive était déjà dépassé. Vous avez raison, mais le Gouvernement déposera un amendement en séance pour réduire le délai transitoire et accélérer la transposition.

En l'état actuel de la rédaction, les dispositions doivent entrer en vigueur en août 2019. L'amendement vise à raccourcir la période transitoire de huit mois, pour une entrée en vigueur en janvier ou février 2019.

Mme Véronique Louwagie. Mais la vérité est qu'elle est déjà dépassée… Ces huit mois n'apportent pas de réponse.

M. le président Éric Woerth. La directive n'est pas dépassée. Elle va dans le sens d'une sécurisation et d'une mise au clair, afin d'éviter que des personnes mal intentionnées ne se servent, en votre nom, de toutes ces données sans véritable régulation. Pour autant, la directive n'aborde effectivement pas les sujets qui ont émergé au cours des trois ou quatre dernières années.

Mme la rapporteure. J'ajouterai que l'ACPR peut moduler les normes techniques. Par ailleurs, madame Pires Beaune, l'ACPR s'engage à réallouer ses ressources pour mettre en œuvre la directive.

M. Jean Lassalle. Cette intervention est passionnante et votre manière de diriger notre commission magnifique, monsieur le président : vous laissez parler tout le monde, y compris les députés de troisième ou quatrième plan !

Ce débat permet de poser une des grandes questions de notre temps, peut-être l'une de celles à l'origine de tant d'angoisse et de stress chez les puissants et les faibles : dans quel paradigme allons-nous enfin trouver un peu de sécurité ?

Il y a quelques jours, j'ai discuté avec un éminent spécialiste, M. Marc Lassus, inventeur et diffuseur mondial de la carte à puce. Il a réalisé une démonstration avec mon téléphone, qui m'a laissé pantois, et expliqué comment les constructeurs étaient tenus de conserver vos données en mémoire – peut-être pas éternellement, mais suffisamment longtemps. Personne ne peut rien contre cela – même pas moi –, même si vous essayez de protéger votre téléphone. Il paraît d'ailleurs que M. Macron en dispose d'un sur-mesure.

Comment peut-on se protéger puisqu'on est toujours dépassé par la technologie, que les textes ont du mal à rattraper ? Je veux donc simplement vous encourager, monsieur le président, et inciter Mme la rapporteure à continuer de travailler, car j'ai besoin de vos lumières. Si vous avez besoin des miennes, vous savez où me trouver. Je ne coûte pas cher, mais je n'apporte pas grand-chose non plus…

Mme Véronique Louwagie. J'entends vos arguments quant aux délais et à l'amendement du Gouvernement accélérant la mise en application à janvier 2019. Pourquoi ne serait-elle pas encore plus rapide si l'on est déjà presque dépassé ?

En novembre 2017, après un certain nombre de discussions entre la Commission européenne et l'Autorité bancaire européenne, il semble que la Commission a adopté un règlement délégué qui, à l'heure actuelle, n'est pas publié. Ce règlement confère force obligatoire aux normes techniques proposées par l'Autorité bancaire européenne en matière d'authentification renforcée. Pouvez nous éclairer à ce sujet ? A priori, même au niveau européen, quelques interrogations persistent…

Mme la rapporteure. Ce projet de règlement a été proposé, mais, normalement, il ne sera adopté que fin février. Je m'efforcerai d'apporter des précisions lors de la séance publique.

Mme Véronique Louwagie. Ce serait intéressant car si, au niveau européen, on s'est rendu compte que des problèmes persistaient pour un certain nombre de dispositifs d'authentification, il faudrait que l'Assemblée nationale en prenne connaissance, pour y apporter des réponses dans le cadre de la transposition.

EXAMEN DES ARTICLES

Article 1er

Ratification de l'ordonnance n° 2017-1252 du 9 août 2017 portant transposition de la directive 2015/2366 concernant les services de paiement dans le marché intérieur

Le présent article ratifie l'ordonnance n° 2017-1252 du 9 août 2017 portant transposition de la directive 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur.

Conformément à l'article 70 de la loi du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique, l'ordonnance précitée comporte, d'une part, des dispositions visant à transposer la directive et, d'autre part, des dispositions permettant l'application et l'adaptation du code monétaire et financier en Nouvelle-Calédonie, en Polynésie française, à Wallis-et-Futuna et dans les collectivités de Saint-Barthélemy, de Saint-Martin et de Saint-Pierre-et-Miquelon.

I. L'ÉLABORATION D'UN CADRE JURIDIQUE AUX ACTIVITÉS DE DEUX NOUVEAUX ACTEURS : LES SERVICES D'INITIATION DE PAIEMENT ET LES SERVICES D'INFORMATION SUR LES COMPTES

L'impératif de rénovation du droit dérivé applicable aux services de paiement tenait en particulier aux évolutions technologiques, aux innovations de procédés et aux innovations de produits touchant ces secteurs. Elles se caractérisent par l'apparition d'acteurs offrant des prestations d'un type nouveau qui, en l'espace de quelques années, ont éprouvé la réglementation en introduisant des incertitudes juridiques concernant la protection des données des utilisateurs et les régimes de responsabilité des prestataires.

Ces entreprises, appartenant souvent à un ensemble que l'on regroupe sous le terme générique de « *Fintech* », constituent un défi pour les acteurs traditionnels comme les établissements de crédit, dans la mesure où elles les obligent à adapter leurs politiques de relations avec les clients. Elles constituent toutefois une source d'opportunités en ce qu'elles favorisent le développement et la diffusion de leurs produits.

La reconnaissance juridique des SIP et des SIC contribue au développement de l'innovation et de la concurrence au sein des secteurs des services de paiement, tout en garantissant une meilleure sécurité juridique, par la définition des droits et obligations afférents à l'exercice de ces activités.

Après la publication de la directive, il revenait au législateur de la transposer. Si le droit interne se conformait pour une grande part aux dispositions de la directive, des adaptations ont toutefois été nécessaires.

A. LA DÉFINITION DES SERVICES D'INITIATION DE PAIEMENT ET DES SERVICES D'INFORMATION DE PAIEMENT

L'article 6 de l'ordonnance modifie l'article L. 314-1 du code monétaire et financier en ajoutant à la liste des services de paiement qu'il dresse les SIP et les SIC. Leur introduction dans le droit européen s'est naturellement accompagnée de règles concernant l'accès aux comptes de paiement, figurant aux articles 66 et 67 de la directive.

1. La création des services d'initiation de paiement et des services d'information sur les comptes

L'article L. 522-1 définit les PSIC comme les personnes, autres que les établissements de crédit, les établissements de monnaie électronique et les établissements de paiement, qui fournissent, à titre de profession habituelle, un service d'information sur les comptes. L'exclusion des PSIC du champ des établissements de paiement se traduit notamment par les différences de règles concernant les conditions d'exercice qui leur sont applicables. Ainsi, conformément à l'article 33 de la directive, les PSIC ne sont pas soumis à un agrément. Un simple enregistrement suffit à l'exercice de leur activité. La directive souligne cependant que, de manière générale, les PSIC sont « *traités comme des établissements de paiement* » (article 33.2).

À la différence des PSIC, l'article L. 522-1 ne définit pas les PSIP. Cette absence s'explique par la distinction qu'opère l'article entre les établissements de paiement, d'une part, et les PSIC, d'autre part. À la différence des PSIC, les PSIP appartiennent à l'ensemble des établissements de paiement, se distinguant des autres établissements par la nature de leur activité. La distinction explicitée se traduit notamment par des conditions d'exercice contraignant inégalement les acteurs, en cohérence avec la directive et avec le niveau de risques que comporte leur activité.

La création d'un statut juridique aux PSIP et aux PSIC s'accompagne de principes cardinaux. Le 32° de l'article 32 de l'ordonnance introduit dans le code monétaire et financier la section 13 « *Modalités d'accès aux comptes de paiement* » dans le chapitre III du titre III du livre I^er^. Les articles L. 133-40 et L. 133-41 de cette section disposent que :

– tout payeur peut s'adresser au PSIP de son choix pour obtenir un service d'initiation de paiement ;

– tout utilisateur de services de paiement peut accéder aux données de ses comptes de paiement par l'intermédiaire d'un PSIC.

Le code monétaire et financier précise d'ailleurs (IV de l'article L. 133-40 et IV de l'article L. 133-41) que ces deux activités existent en dehors de tout contrat avec le gestionnaire des comptes, transposant ainsi les dispositions des articles 66.4 et 67.4 de DSP 2.

2. L'adaptation des règles existantes aux opérations dans lesquelles intervient un prestataire de services de paiement

Contrairement aux PSIC, les PSIP interviennent dans la procédure d'exécution du paiement. Certaines règles européennes déjà applicables à des prestataires de services de paiement leur ont été étendues. L'ordonnance tire toutes les conséquences de l'introduction de ce nouveau type d'acteurs dans le droit européen en adaptant le code monétaire et financier.

● La règle selon laquelle l'opération de paiement est subordonnée au consentement du payeur donné à son prestataire est modifiée afin de prévoir que le payeur peut donner son **consentement** à son PSIP, conformément à l'article 64.2 de la directive. Le 8° de l'article 2 de l'ordonnance insère un alinéa à l'article L. 133-7 du code monétaire et financier à cet effet.

De même, la **règle d'irrévocabilité d'un ordre de paiement** une fois que le payeur a donné son consentement est étendue aux opérations dans lesquelles intervient un PSIP, par la modification de l'article L. 133-8, dans sa version résultant du 9° de l'article 2 de l'ordonnance, conformément aux dispositions de l'article 80.2 de la directive.

Enfin, l'obligation qui incombe au prestataire de services de paiement de **notifier à l'utilisateur son refus d'exécuter un ordre de paiement** est étendue aux PSIP, par la modification de l'article L. 133-10, en conformité avec l'article 79 de la directive.

● Il était également nécessaire de modifier le code monétaire et financier afin d'adapter le **régime de responsabilité** des services de paiement au cas **d'opérations non autorisées** réalisées par un PSIP. À cette fin, l'article L. 133-18, modifié par le 19° de l'article 2 de l'ordonnance, reprend les termes de l'article 73 de la directive pour le transposer.

En premier lieu, la règle selon laquelle toute opération non autorisée, signalée par l'utilisateur à son prestataire de services de paiement, donne lieu à un remboursement immédiat au payeur du montant de l'opération connaît deux aménagements. D'une part, la nouvelle rédaction précise que le **remboursement a lieu immédiatement** après que le prestataire a pris connaissance de l'opération et « *en tout état de cause* ***au plus tard à la fin du premier jour ouvrable suivant*** », alors que l'article L. 133-18 dans sa version antérieure à l'ordonnance se bornait à préciser que le remboursement était immédiat. D'autre part, le prestataire de services de paiement doit se soustraire à cette obligation s'il a de bonnes raisons de soupçonner une fraude de l'utilisateur, auquel cas il doit communiquer les raisons de ses soupçons, par écrit, à la Banque de France.

En second lieu, l'article L. 133-18 modifié prévoit le cas où l'opération de paiement non autorisée est initiée par un PSIP en déterminant le circuit des éventuels remboursements ou indemnisations.

Celui-ci charge d'abord le gestionnaire de compte du remboursement immédiat et au plus tard à la fin du premier jour ouvrable suivant l'opération du remboursement au payeur, étant précisé que la date de valeur à laquelle le compte de paiement du payeur est crédité ne peut être postérieure à la date à laquelle le compte a été débité.

Dans un second temps, si la responsabilité de l'opération non autorisée revient au PSIP, ce dernier indemnise immédiatement le gestionnaire du compte, à sa demande. Il est précisé que l'indemnisation vaut pour les pertes subies ou les sommes payées en raison du remboursement du payeur, y compris le montant de l'opération de paiement non autorisée.

● Parallèlement aux modifications du régime de responsabilité en cas d'opérations non autorisées, les dispositions qui régissent les **situations où un utilisateur nie avoir autorisé une opération exécutée ou affirme qu'une opération a été mal exécutée** sont également adaptées aux opérations initiées par des PSIP. L'article L. 133-23 du code monétaire et financier disposait (en conformité avec l'actuel article 72 de la directive) qu'il appartient au prestataire de services de paiement de prouver que l'opération a été :

– authentifiée ;

– dûment enregistrée et comptabilisée ;

– qu'elle n'a pas été affectée par une déficience technique ou autre.

Le seul fait que l'opération a été dûment enregistrée n'emporte pas la preuve que le payeur l'a autorisée ou qu'il n'a pas satisfait, par négligence grave ou de manière intentionnelle, à ses obligations.

Le 26° de l'article 2 de l'ordonnance crée l'article L. 133-23-1 du code monétaire et financier précise que **lorsque l'opération en question a été initiée par un PSIP, c'est à lui qu'il revient de prouver que l'ordre de paiement a été reçu par le gestionnaire du compte du payeur et que, « *pour ce qui le concerne* »**, l'opération respecte les trois critères présentés ci-dessus, conformément à l'article 72.2 de la directive.

● Transposant les dispositions de l'article 90 de la directive, le 24° de l'article 2 de l'ordonnance, qui introduit les articles L. 133-22-1 et L. 133-22-2 dans le code monétaire et financier, prévoit des règles de remboursement et d'indemnisation similaires en ce qui concerne les **opérations mal exécutées, non exécutées ou exécutées tardivement**, lorsqu'elles ont été initiées par un PSIP. Ces dispositions ne s'appliquent pas :

– lorsque l'utilisateur a fourni un identifiant unique inexact, ce qui a entraîné la mauvaise exécution de l'opération (article L. 133-21). En effet, en pareils cas, le PSIP n'est pas responsable de la mauvaise exécution de l'opération ;

– lorsque l'utilisateur, dûment informé par son PSIP, ne l'a pas signalé dans un délai de treize mois (ce délai peut être distinct pour les personnes morales ou pour les professionnels si les parties le décident), en vertu de l'article L. 133-24 du code monétaire et financier, tel que modifié par le 27° de l'article 2 de l'ordonnance.

B. LES DROITS ET OBLIGATIONS DES SERVICES D'INITIATION DE PAIEMENT ET DES SERVICES D'INFORMATION SUR LES COMPTES

L'accès aux comptes de paiement constitue l'un des enjeux les plus importants de la transposition de la directive. D'ailleurs, ses dispositions qui y ont trait ne seront applicables qu'à l'issue d'une période de transition, selon son article 115.4. Comme mentionné à plusieurs reprises, elles entreront en vigueur à l'expiration d'un **délai de dix-huit mois suivant la publication du règlement dérivé** fixant les normes techniques de réglementation régissant en particulier les communications entre les gestionnaires de compte, les PSIP et les PSIC.

1. L'accès aux comptes de paiement : un principe de communication dont les enjeux résident dans l'application technique

a. Des principes de communication sécurisée entre les gestionnaires de compte, les PSIP et les PSIC

Les dispositions de la directive concernant les modalités d'accès aux comptes de paiement figurent parmi les plus importantes, en ce qu'elles fixent le cadre des relations entre les acteurs traditionnels et les nouveaux services de paiement.

● La directive exige l'**application du principe de non-discrimination à l'accès des prestataires de services de paiement aux systèmes de paiement** [(1)], y compris à ceux qui ne sont pas des participants à ce système de paiement, afin qu'ils puissent transmettre des ordres de transfert par l'intermédiaire de ce système. Ainsi, l'article 35 de la directive dispose que lorsqu'un participant à un système de paiement permet à un prestataire tiers au système de transmettre des ordres, il doit offrir cette même possibilité, sur demande, aux autres prestataires dans la même situation. En cas de refus, celui-ci doit être motivé.

● Les articles 66 et 67 de la directive garantissent l'existence des activités d'initiation de paiement et d'information sur les comptes en dehors de toute relation contractuelle entre les gestionnaires de compte et les PSIP d'une part,

(1) Un système de paiement est défini comme « un système permettant de transférer des fonds régi par des procédures formelles standardisées et des règles communes pour le traitement, la compensation et/ou *le règlement d'opérations de paiement »*, selon l'article 4 de la directive DSP 2.

entre les gestionnaires de compte et les PSIC d'autre part. De ce principe découlent un certain nombre d'obligations des gestionnaires de compte à l'endroit des PSIP et des PSIC.

Vis-à-vis des PSIP, les gestionnaires de compte sont tenus de mettre à leur disposition toutes les informations sur l'**initiation des opérations de paiement** et toutes les informations auxquelles ils ont eux-mêmes accès sur l'**exécution des opérations de paiement**. Ils doivent, de plus, traiter les ordres de paiement transmis par l'intermédiaire des PSIP sans discrimination autre que celle fondée sur des critères objectifs, en termes de délai, de priorité ou de frais, par rapport aux ordres de paiement transmis directement par les payeurs. Le III de l'article L. 133-40, créé par l'article 2 de l'ordonnance, a transposé ces dispositions.

Vis-à-vis des PSIC, les gestionnaires de compte doivent **traiter les demandes de données** transmises grâce à leurs services sans discrimination autre que celle fondée sur des raisons objectives.

● Les gestionnaires de compte sont également soumis à une obligation essentielle : ils doivent **communiquer de manière sécurisée avec ces deux types d'acteurs**, selon le a) de l'article 66.4 et le a) de l'article 67.4. Les modalités de cette communication doivent entrer en conformité avec les NTR évoquées *supra*, dont les modalités d'élaboration sont déterminées par l'article 98.1 de la directive. Les articles L. 133-40 (pour les PSIP) et L. 133-41 (pour les PSIC) du code monétaire et financier, créés par le 32° de l'article 2 de l'ordonnance, donnent une valeur législative à ces dispositions de droit dérivé.

● Dans le cadre de l'exercice de leurs activités, les PSIP et les PSIC doivent de plus **s'identifier auprès des gestionnaires de compte**. Chaque fois qu'un paiement est initié, le PSIP qui en est à l'origine doit s'identifier auprès du gestionnaire du compte (article 66.3 transposé par le 4° du II de l'article L. 133-40). De la même manière, le PSIC doit s'identifier auprès des gestionnaires des comptes de l'utilisateur de ses services pour chaque session de communication (article 67.2 transposé par le 3° du II de l'article L. 133-41).

Dans le cadre des obligations d'**authentification forte**, l'article 97 de la directive exige du gestionnaire du compte qu'il autorise le PSIP ou le PSIC à s'appuyer sur les procédures qu'il a mises en place à destination de ses clients. Si l'obligation d'application de l'authentification forte n'entre en vigueur qu'au terme de la période de transition évoquée, les gestionnaires sont toutefois déjà tenus de permettre aux PSIP et aux PSIC d'accéder à leur procédure d'authentification, avant l'entrée en vigueur pleine et entière de l'article 98. Il n'est pas précisé que l'authentification doit être forte, conformément à l'article L. 133-44. Les PSIP et PSIC doivent donc pouvoir continuer à accéder aux données bancaires durant la période de transition, sans que l'obligation de s'identifier s'impose à eux.

● Le principe du droit, pour ces deux types de prestataires, à un accès au compte de paiement de l'utilisateur connaît des restrictions. Il demeure possible pour le gestionnaire du compte de refuser l'accès à ces prestataires dès lors qu'il a des « *raisons objectivement motivées ou documentées liées à un accès non autorisé ou frauduleux au compte de paiement* » de la part du prestataire en question, « *y compris l'initiation non autorisée ou frauduleuse d'une opération de paiement* », aux termes du nouvel article L. 133-17-1 de la nouvelle sous-section 2 « *Relation entre les prestataires de services de paiement respectivement parties avec l'utilisateur de services de paiement* » de la section 5 du chapitre III du titre III du livre I^{er} du code monétaire et financier, introduit par le 18° de l'article 2 de l'ordonnance et reprenant les termes de l'article 68.5 de la directive.

Dans ce cas, le gestionnaire du compte a obligation d'informer de ce refus :

– le payeur si possible avant que l'accès soit refusé et, au plus tard, immédiatement après ;

– la Banque de France, immédiatement. Si elle l'estime pertinent, cette dernière peut notifier l'incident à l'Autorité de contrôle prudentiel et de résolution (ACPR).

Une fois que ces raisons motivées et documentées n'existent plus, l'accès au compte est rétabli.

b. Une application technique aux enjeux fondamentaux

En conférant un statut juridique aux PSIP et aux PSIC, la directive a entendu non seulement favoriser l'innovation dans le secteur des services de paiement, mais également conférer une plus grande sécurité juridique à leurs activités. Elle reconnaît en effet aux PSIP et aux PSIC la possibilité d'accéder aux comptes de paiement, mais encadre les modalités de leur accès.

Si elle fixe le cadre général de la communication entre les gestionnaires de compte, les PSIP et les PSIC, **c'est dans l'application technique de ces principes que le point d'équilibre entre l'objectif de soutien à l'innovation et à la concurrence d'une part, et la garantie de la sécurité des données d'autre part, doit désormais être trouvé.**

i. Les enjeux liés à l'accès des PSIP et des PSIC aux données des comptes de paiement

Par leur nature, conjuguée à l'apparition ou au développement de nouvelles formes de services de paiement, à la multiplicité des acteurs et à l'accélération de la circulation des données, l'accès aux données des comptes de paiement comporte des risques en matière de sécurité des données personnelles et de respect de la vie privée. Tant les établissements de crédit que les acteurs de la *Fintech* sont confrontés à ces risques, eu égard à la grande diversité des données

collectées, à leur sensibilité et à leur nombre. Elles sont convoitées, l'analyse de certaines d'entre elles permettant une connaissance fine des habitudes de consommation des utilisateurs, par exemple.

L'évolution technologique dans l'environnement des services de paiement et, partant, les nouvelles formes d'activité, participent à l'amplification de ces risques communs au secteur. Néanmoins, des risques spécifiques s'attachent aux activités des *Fintech* (1).

Actuellement, les PSIC ou les PSIP accèdent aux comptes des utilisateurs par la technique du *screen scraping* non identifié, expliquée dans la partie *Exposé générale*. Elle consiste en l'utilisation de robots qui permettent aux PSIP et aux PSIC d'accéder aux données de leurs clients sur l'espace personnel en ligne que les gestionnaires de compte mettent à leur disposition et de les extraire. Actuellement, l'accès se fait au moyen de la communication par l'utilisateur aux PSIP et aux PSIC de ses codes d'accès. Il ne s'agit pas d'un problème lié à la technique elle-même, mais aux modalités d'authentification.

Cette technique, généralement proscrite par les établissements bancaires dans leurs conditions d'utilisation, comporte des incertitudes juridiques. Elle pose également question quant à la sécurité des données des utilisateurs et au champ pertinent des données auxquelles les PSIC doivent avoir accès. Impliquant l'accès d'un tiers aux données personnelles des clients, plusieurs difficultés en découlent (2). Elles concernent notamment :

– l'exigence de consentement libre et expresse de la renonciation de l'utilisateur au secret bancaire (3) ;

– le respect du principe de finalité de la collecte et du traitement des données (4), qui restreint l'utilisation de ces données à des fins commerciales ;

– la sécurité des données, compte tenu de leur exposition au risque de fraude.

Toutefois, on constate que cette technique d'accès aux données, utilisée depuis plusieurs années par certains PSIP, n'a pas eu de conséquence majeure, pour ce que l'on sait, concernant la sécurité des données des utilisateurs. En tout état de cause, les dispositions de la directive DSP 2 contribuent à renforcer la sécurité des données des utilisateurs. Elles devront toutefois trouver leur traduction technique par l'intermédiaire d'un règlement délégué et dans le droit interne.

---

(1) Juliette Morel-Maroger, L'apport des Fintech au droit bancaire : les nouveaux risques. La protection de la vie privée et des données personnelles de l'usager du secteur bancaire, *Revue de Droit bancaire et financier, n° 1, janvier 2017.*

(2) Ibidem.

(3) Conseil d'État, 30 décembre 2009, Société Experian*, n° 306173.*

(4) Article 6 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

ii. L'application des normes techniques de réglementation dans le droit interne

● Comme indiqué *supra*, la communication entre les gestionnaires de compte, les PSIP et les PSIC doit satisfaire des normes techniques de réglementation dites « NTR », conformément aux prescriptions de l'article 98 de la directive. Ce dernier renvoie à l'Autorité bancaire européenne (ABE) le soin d'élaborer des projets de NTR, « *en collaboration avec la BCE et après avoir consulté toutes les parties concernées* ».

Sur la base de cette proposition, la Commission a été habilitée par l'article 98.2 à prendre un acte délégué pour déterminer ces normes.

Suivant ces dispositions, l'ABE a procédé à une consultation qui s'est achevée le 12 octobre 2016. Elle a publié son projet final le 23 février 2017 [(1)]. La Commission lui a notifié le 24 mai 2017 sa lettre d'intention d'amender le projet [(2)], lettre sur laquelle l'ABE a émis son opinion, publiée le 29 juin 2017 [(3)]. **Enfin, le 27 novembre 2017, la Commission a publié un projet de règlement délégué tenant compte des observations de l'ABE**.

● Selon ce projet, l'échange d'informations entre les gestionnaires, les PSIP et les PSIC s'opérerait par l'intermédiaire d'**interfaces standardisées, ouvertes et sécurisées.** Les gestionnaires de compte auraient ainsi l'obligation de développer et de maintenir au moins une interface ouverte aux PSIP et aux PSIC, en vue de l'accès aux informations sur les comptes de paiement. La Commission propose parallèlement d'interdire la pratique du *screen scraping* **non identifié** à l'issue de la période de transition dont la durée a été fixée à dix-huit mois après l'entrée en vigueur des normes techniques de réglementation (article 115.4 de la directive).

Afin de certifier la qualité de l'outil que le gestionnaire de compte met à disposition des PSIP et des PSIC, des indicateurs de performance et des valeurs cibles doivent être prévus par le gestionnaire. Ils devront être aussi exigeants que ceux que le gestionnaire a fixés pour l'interface destinée à ses propres clients. Les résultats devront être trimestriellement publiés.

● La question de l'introduction éventuelle d'un « **mécanisme de secours** » a fait l'objet d'échanges et de propositions entre l'ABE et la Commission européenne. Il s'agissait d'apporter une réponse aux situations de défaillance ou d'indisponibilité de l'interface dédiée, empêchant les PSIP ou les

---

(1) European Banking Authority, *Draft Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2)*, 23 February 2017.

(2) *http://www.eba.europa.eu/documents/10180/1806975/%28EBA-2017-E-1315%29%20Letter+from+O+Guersent%2C%20FISMA+re+Commission+intention+to+amend+the+draft+RTS+on+SCA+and+CSC+-Ares%282017%292639906.pdf/efbf06e1-b0e9-4481-88e5-b70daa663cb9*

(3) European Banking Authority, *Opinion of the European Banking Authority on the European Commission's intention to partially endorse and amend the EBA's final draft regulatory technical standards on strong customer authentication and common and secure communication under PSD2*, 29 June 2017.

PSIC d'exercer leur activité. La Commission avait initialement proposé d'ouvrir les interfaces destinées aux clients des banques en tant que canal de communication sécurisé pour les PSIP et les PSIC, dans des conditions respectant les articles 65 à 67 de la directive, régissant les modalités d'accès aux comptes des prestataires tiers.

Toutefois, l'ABE a émis un avis négatif sur ce système pour deux raisons :

– le coût d'un tel mécanisme pour les gestionnaires de comptes ;

– le risque d'aléa moral, les gestionnaires n'étant pas incités à développer les API si un mécanisme de secours est prévu.

Tenant compte de cet avis, la Commission a révisé son projet. Désormais, le projet prévoit toujours le principe d'un mécanisme de secours. Toutefois, la Commission habiliterait les autorités nationales compétentes à exempter les banques de l'obligation de prévoir ce mécanisme si des conditions strictes sont remplies, garantissant que les interfaces ouvrent réellement le marché des services de paiement. **Elles seront soumises à un test de résistance par les PSIP et contrôlées par les autorités compétentes. En cas d'échec au test, les PSIP pourront recourir au mécanisme d'urgence**.

En France, ces interfaces pourraient prendre la forme d'API. Il s'agit d'une solution informatique qui facilite, *via* un langage de programmation, l'accès aux services d'une application.

Durant la période de transition, le X de l'article 34 de l'ordonnance prévoit que les **gestionnaires « *ne peuvent se prévaloir de* [la] *non-conformité* [des interfaces] *pour bloquer ou entraver l'utilisation de services d'initiation de paiement et de services d'information sur les comptes pour les comptes dont ils sont gestionnaires* »**.

● Le projet de règlement précise que ces dispositions sur l'accès à l'information **ne concernent que les comptes de paiement**. Il ne modifie pas les règles d'accès aux comptes qui ne sont pas des comptes de paiement, ces règles ressortissant à la compétence des États membres. Autrement dit, le législateur est libre d'adopter des règles similaires concernant les comptes d'épargne, d'assurance vie ou les comptes titres, mais rien ne l'y oblige (voir la partie *Exposé général,* III. B.).

2. La transposition des obligations des services d'initiation de paiement et des services d'information sur les comptes

Aux statuts nouvellement créés de PSIP et de PSIC s'attachent des obligations et des interdictions que l'ordonnance transpose dans le code monétaire et financier.

● Les articles 66 et 67 de la directive listent deux séries d'obligations et d'interdictions applicables respectivement aux PSIP et aux PSIC. Le 32° de l'article 2 de l'ordonnance a créé les articles L. 133-40 et L. 133-41 dans le code monétaire et financier.

S'agissant de la **protection des données de sécurité personnalisées des utilisateurs**, tant les PSIP que les PSIC doivent veiller à ce qu'elles ne soient pas accessibles à d'autres parties que les utilisateurs et les émetteurs de ces données. Les PSIP doivent veiller à transmettre ces données au moyen de canaux « *sûrs et efficaces* » (article L. 133-40) et les PSIC doivent veiller à les transmettre « *de manière sécurisée* » (article L. 133-41).

Une **obligation d'identification** incombe à chacun des deux types de prestataires, lors de l'exercice de leur activité. Ainsi, les PSIP doivent s'identifier auprès du gestionnaire du compte payeur chaque fois qu'un paiement est initié, tandis que l'exigence d'identification des PSIC s'impose à eux à chaque session de communication auprès des gestionnaires des comptes de l'utilisateur. Dans l'un et l'autre cas, ces communications doivent répondre aux exigences des NTR (voir *supra*).

Cette obligation d'identification n'entre en vigueur qu'à l'issue de la période de transition, en vertu de l'article 34 de l'ordonnance. Autrement dit, les PSIP et les PSIC pourront continuer à utiliser le *web scraping* sans s'identifier, tant que la période de transition ne sera pas expirée.

● Les obligations et interdictions des PSIP et des PSIC relatives au champ des données disponibles et à leur usage diffèrent compte tenu de leurs spécificités. Un principe général leur est toutefois commun : **ils ne peuvent utiliser, consulter ou stocker des données qu'aux seules fins de leur activité**.

Il est fait interdiction aux PSIP de stocker des données de paiement sensibles concernant l'utilisateur. Ils ne peuvent pas non plus demander à l'utilisateur des données **autres que celles nécessaires pour fournir le service d'initiation de paiement**. Dans le même esprit, les PSIC ne peuvent accéder qu'aux informations provenant des comptes de paiement indiqués par l'utilisateur et ils ont **interdiction de demander des données de paiement sensibles liées à des comptes de paiement**.

● Des obligations supplémentaires s'imposent aux PSIP. Tout d'abord, ils ne peuvent détenir à aucun moment les fonds du payeur ayant fait l'objet des opérations de paiement qu'ils ont initiées. Ensuite, ils sont chargés de veiller à ce que toute information relative aux utilisateurs de services de paiement qu'ils ont obtenue lors de leur prestation ne soit communiquée qu'au bénéficiaire du paiement et avec le consentement exprès de l'utilisateur. Enfin, interdiction leur est faite de modifier le montant, le bénéficiaire ou tout autre caractéristique de l'opération de paiement.

● L'article 5.2 de la directive impose tant aux PSIP qu'aux PSIC qu'ils disposent **d'une assurance de responsabilité civile professionnelle**, ce que l'article 13 de l'ordonnance a transposé par la création de l'article L. 522-1-1. Il est précisé que l'assurance des PSIC couvre leur responsabilité vis-à-vis des gestionnaires des comptes ou des utilisateurs à la suite d'accès non autorisés aux données des comptes de paiement ou de leur utilisation non autorisée. Les critères permettant de déterminer le montant minimal de l'assurance relèvent d'une précision par arrêté. Celle-ci a été opérée par la publication de l'arrêté du 31 août 2017 qui a introduit l'article 5-1 dans l'arrêté du 29 octobre 2009 portant sur la réglementation prudentielle des établissements de paiement.

● Compte tenu de la nature de leur activité, les SIC ne sont pas soumis aux dispositions du chapitre III du titre III du livre I^{er} du code monétaire et financier fixant les règles applicables aux instruments de paiement, contrairement aux autres services de paiement. Leur sont toutefois appliquées :

– la règle selon laquelle l'utilisateur de ces services doit prendre toute mesure raisonnable pour préserver la sécurité de ses données de sécurité personnalisées (article L. 133-16) ;

– l'obligation pour l'utilisateur de respecter des conditions de délivrance et d'utilisation des moyens de paiement, lesquelles doivent être objectives, non discriminatoires et proportionnées (article L. 133-16).

● Le droit européen [(1)] et le droit national [(2)] prévoient un certain nombre d'obligations, applicables notamment aux prestataires de services de paiement, en matière de **lutte contre le blanchiment de capitaux et le financement du terrorisme**. La directive DSP 2 précise que ces règles ne font pas partie des normes auxquelles il peut être dérogé sur le critère de volume des opérations de paiement exécutées, au titre de son article 32. En revanche, elle ne précise pas que les PSIP ou les PSIC sont soumis à ces règles. L'article L. 561-2-3 exempte les prestataires de services de paiement, pour la seule activité de PSIC, des dispositions du code monétaire et financier relatives à la lutte contre le blanchiment des capitaux et le financement du terrorisme.

Dans la même logique, l'article L. 561-9 étend aux services de paiement présentant un faible risque de blanchiment de capitaux ou de financement du terrorisme la possibilité de mettre en œuvre des mesures de vigilance simplifiée. Les conditions d'application de cette souplesse sont toutefois strictes. Elles étaient déjà en vigueur pour les personnes ou les produits présentant un faible risque concernant ces menaces et sont précisées à l'article R. 561-16-1 du code monétaire et financier.

---

(1) Directive (UE) 2015/849 du Parlement européen et du Conseil du 20 mai 2015 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, modifiant le règlement (UE) n° 648/2012 du Parlement européen et du Conseil et abrogeant la directive 2005/60/CE du Parlement européen et du Conseil et la directive 2006/70/CE de la Commission.

(2) Titre VI du livre V du code monétaire et financier.

II. L'EXTENSION DU CHAMP D'APPLICATION DES RÈGLES APPLICABLES AUX SERVICES DE PAIEMENT

L'article 2 de l'ordonnance tire les conséquences dans le code monétaire et financier de l'extension du champ d'application territorial des règles du droit dérivé concernant les services de paiement. Elle introduit également dans le code monétaire et financier certaines définitions prévues par la directive.

A. LE CHAMP D'APPLICATION TERRITORIAL

1. Le champ d'application territorial de DSP 2

La directive a étendu le champ d'application des règles qu'elle édicte au-delà du territoire de l'Union européenne et de l'Espace économique européen, en distinguant trois cas de figure.

Lorsque les prestataires de services du paiement en question sont situés dans l'Union européenne, l'opération de paiement se voit appliquer l'ensemble des dispositions de la directive relatives à la transparence des conditions et les exigences en matière d'information (titre III de la directive) d'une part, et aux droits et obligations liés à la prestation et à l'utilisation de services de paiement (titre IV de la directive) d'autre part.

Lorsqu'une opération de paiement est effectuée dans une devise qui n'est pas celle d'un État membre et que les prestataires de services du paiement sont situés dans l'Union européenne, sont applicables les dispositions relatives :

– à la transparence des conditions et aux exigences en matière d'informations (titre III), sauf les dispositions concernant l'information de l'utilisateur sur le délai d'exécution maximal de fourniture du service de paiement (b) de l'article 45.1 ; 2) e) de l'article 52 ; a) de l'article 56) ;

– aux droits et obligations liés à la prestation de paiement (titre IV), sauf les règles concernant : la perception de frais sur le montant transféré (article 81) ; les opérations de paiement effectuées vers un compte de paiement (article 83) ; le cas dans lequel le bénéficiaire n'est pas titulaire d'un compte de paiement auprès du prestataire de services de paiement (article 84) ; les espèces déposées sur un compte de paiement (article 85) ; les opérations de paiement national (article 86).

Enfin, quelle que soit la devise utilisée, dès lors que l'un des prestataires se situe dans l'Union européenne, les parties de l'opération de paiement qui sont effectuées dans l'Union européenne sont soumises à un socle de règles qui se distingue de celui applicable au cas précédent par la non-application des règles de partage de frais entre le prestataire du bénéficiaire et celui du payeur et des règles de remboursement d'opérations initiées par le bénéficiaire.

2. Les modifications du champ d'application territorial dans le code monétaire et financier

L'ordonnance du 9 août 2017 a tiré les conséquences de l'extension du champ territorial d'application de la directive dans les domaines qu'elle recouvre.

a. Le champ d'application territorial des règles relatives aux instruments de paiement et à l'accès aux comptes

L'article L. 133-1 du code monétaire et financier soumettait les opérations de paiement aux règles du code applicables aux instruments de paiement (chapitre III du titre III du livre I^{er}), dès lors que :

– l'un des prestataires de services de paiement du bénéficiaire ou du payeur se situait en France hexagonale, dans l'une des collectivités de l'article 73 de la Constitution, à Saint-Martin, à Saint-Barthélemy ou à Saint-Pierre-et-Miquelon et l'autre dans un État de l'espace économique européen (y compris la France) ;

– l'opération de paiement était réalisée en euros ou dans la devise d'un État de l'Espace économique européen.

Tirant les conséquences de l'extension territoriale prévue par la directive, le 2° de l'article 2 de l'ordonnance du 9 août 2017 a modifié l'article L. 133-1 en prévoyant trois niveaux d'application des dispositions du **chapitre III du code monétaire et financier qui correspondent aux trois niveaux présentés par l'article 2 de la directive**. Par ailleurs, Saint-Barthélemy et Saint-Pierre-et-Miquelon ne sont plus mentionnés dans l'article L. 133-1 tel qu'il résulte de l'ordonnance, le régime d'application de ces dispositions dans ces territoires faisant l'objet d'une modification de l'article L. 133-1-1. Saint-Barthélemy, qui relevait uniquement de l'article L. 133-1 est passée sous le régime de l'article L. 133-1-1.

En premier lieu, l'ensemble des dispositions du chapitre III est applicable si :

– les prestataires de services de paiement du bénéficiaire et du payeur se situent, l'un en France métropolitaine, dans l'une des collectivités de l'article 73 de la Constitution ou à Saint-Martin et l'autre dans l'Union européenne ;

– la devise utilisée est celle d'un pays de l'Union européenne ou d'un État partie à l'accord sur l'Espace économique européen.

En deuxième lieu, les dispositions du chapitre III à l'exception de celles relatives à l'interdiction de prélèvement de frais sur le montant de l'opération de paiement, du délai d'exécution de paiement et de la date de valeur sont applicables si :

– les prestataires répondent au même critère de territorialité que le cas précédent ;

– l'opération est réalisée dans la devise d'un État qui n'appartient pas à l'accord sur l'Espace économique européen.

En troisième et dernier lieu, les dispositions du chapitre III à l'exception de celles relatives à l'interdiction de prélèvement de frais sur le montant transféré, du délai d'exécution du paiement, des règles de responsabilité et de remboursement en cas d'opération mal exécutée, des règles de remboursement d'opérations initiées par le bénéficiaire et de partage des frais entre le prestataire du bénéficiaire et celui du payeur sont applicables dès lors qu'un seul des deux prestataires de paiement du payeur ou du bénéficiaire se situe sur le territoire national, tel que défini plus haut.

L'ordonnance opère également des modifications concernant l'application du chapitre III à deux territoires d'outre-mer. Comme il a été évoqué *supra*, Saint-Barthélemy et Saint-Pierre-et-Miquelon, qui étaient mentionnés à l'article L. 133-1 avant l'entrée en vigueur de l'ordonnance aux côtés des collectivités de l'article 73 de la Constitution et de Saint-Martin, n'y figurent plus.

En revanche, ces deux territoires font l'objet de règles particulières concernant l'application des articles du chapitre III. C'était déjà le cas pour Saint-Pierre-et-Miquelon avant l'intervention de l'ordonnance, qui a ajouté Saint-Barthélemy à ce régime. Cette modification est cohérente avec le changement de statut de Saint-Barthélemy en 2012, vis-à-vis de l'Union européenne. Avant cette date, le territoire avait le statut des régions ultrapériphériques (RUP) ; il répond depuis au régime des Pays et territoires d'Outre-mer (PTOM). Or, les PTOM ne font pas partie du territoire de l'Union européenne, mais font partie du territoire national, ce qui explique le régime dérogatoire qui leur est appliqué.

Dans le cas où le prestataire de services de paiement du payeur est situé dans l'un de ces deux territoires et que le prestataire de services de paiement du bénéficiaire est situé hors de France, quelle que soit la devise utilisée pour l'opération, sont applicables les dispositions relatives aux obligations des parties en matière d'instruments de paiement, notamment s'agissant de la sécurité des données et les dispositions relatives à la responsabilité en cas d'opération de paiement par carte non autorisée.

b. Le champ d'application territorial des règles relatives aux obligations des services de paiement

L'ordonnance du 9 août 2017 a modifié le chapitre IV « *Les services de paiement* » au livre III du code monétaire et financier, afin de transposer les dispositions de la directive relatives aux obligations des services de paiement.

En fonction des localisations géographiques des acteurs et des devises utilisées, deux situations sont possibles :

– si le prestataire de services de paiement du bénéficiaire et celui du payeur se situent, l'un en France hexagonale ou dans l'un des territoires d'outre-mer de l'article 73 de la Constitution ou de Saint-Martin, et l'autre dans un autre État membre de l'Espace économique européen et si l'opération est réalisée dans la monnaie de l'un des États parties à l'Espace économique européen, alors l'ensemble des dispositions relatives aux obligations des services de paiement sont applicables ;

– si un seul des prestataires est situé sur le territoire national tel que défini précédemment, alors, quelle que soit la devise utilisée, les dispositions du chapitre IV sont applicables, à l'exception de celles touchant aux règles de délai d'exécution maximal des opérations, pour ce qui concerne les parties de l'opération de paiement qui sont effectuées dans l'Union.

B. LES ACTEURS ET LES TYPES DE SERVICES CONCERNÉS

● Le champ de la directive est naturellement déterminé par la notion de services de paiement, que l'article 4 de la directive définit comme les activités dont la liste est présentée en annexe I de la directive. L'article L. 314-1 du code monétaire et financier, résultat de l'article 6 de l'ordonnance, reprend cette liste. Il s'agit des activités suivantes :

– les services permettant le versement d'espèces sur un compte de paiement et les opérations de gestion d'un compte de paiement ;

– les services permettant le retrait d'espèces sur un compte de paiement et les opérations de gestion d'un compte de paiement ;

– l'exécution des opérations de prélèvements, de paiement avec carte et de virements ;

– l'émission d'instruments de paiement ou l'acquisition d'opérations de paiement ;

– les services de transmission de fonds ;

– les services d'initiation de paiement ;

– les services d'information sur les comptes.

● L'article 3 de la directive exclut du champ de son application un certain nombre d'activités, ce qui permet de délimiter avec davantage de précision les contours des services de paiement. Le e) dispose que la fourniture de services pour lesquels des espèces sont fournies par le bénéficiaire au bénéfice du payeur dans le cadre d'une opération de paiement, à la demande expresse de l'utilisateur de services de paiement formulée juste avant l'exécution de l'opération de paiement *via* un paiement pour l'achat de biens ou de services n'est pas un service de paiement.

Cette disposition figurait déjà dans la directive DSP 1. **Elle autorise la pratique du *cashback*** (voir *supra*). Aucune disposition ne l'encadre dans le droit interne, ce qui freine la réalisation par les commerçants des investissements nécessaires à son développement et comporte un risque potentiel de fraudes ou de blanchiment.

Une forme de *cashback* existe déjà dans certaines zones dépourvues de distributeurs automatiques de billets. Certaines banques ont en effet développé des partenariats avec des commerces de proximité pour que ces derniers offrent à leurs clients la possibilité de retirer des espèces. Comme expliqué plus haut, le développement du *cashback* est une source d'opportunités à la fois pour les commerçants, pour les utilisateurs des services de paiement et pour les banques.

La rapporteure estime que la pratique, dès lors qu'elle est encadrée, devrait être autorisée.

● Les considérants de la directive indiquent que le développement de l'activité d'émission d'un instrument de paiement lié à une carte par un prestataire de services de paiement, qu'il s'agisse d'une banque, d'un autre établissement de crédit ou d'un établissement de paiement, participerait à renforcer la concurrence sur le marché, ce qui bénéficierait donc au consommateur. Eu égard à la dynamique de l'innovation dans le secteur, de nouveaux canaux de paiement liés à une carte pourraient apparaître. Avec le développement possible de ces modes de paiement apparaissent des enjeux liés à l'information de la disponibilité des fonds sur les comptes des utilisateurs.

Ainsi, l'article 65 de la directive, que le 32° de l'article 2 de l'ordonnance a transposé dans le code monétaire et financier par la création de l'article L. 133-39, impose aux gestionnaires de comptes de confirmer au prestataire de services de paiement émetteur de l'instrument lié à une carte, à sa demande, si le montant nécessaire à l'exécution de l'opération est disponible sur le compte du payeur. Cette confirmation a lieu immédiatement. La réponse du gestionnaire ne porte que sur la disponibilité du montant au moment de la demande. Elle ne peut être stockée ni utilisée à d'autres fins que l'exécution d'une opération de paiement liée à une carte. Elle ne permet pas au gestionnaire de bloquer les fonds sur le compte du payeur.

Trois conditions préalables doivent toutefois être satisfaites pour qu'une opération donne lieu à cette confirmation :

– le compte du paiement du payeur est accessible en ligne au moment de la demande ;

– le payeur a donné son consentement exprès au gestionnaire du compte à ce que la confirmation puisse avoir lieu ;

– le consentement ci-dessus a été donné avant la première demande de confirmation.

La demande de confirmation de l'émetteur de l'instrument de paiement lié à une carte est également soumise au respect de quatre conditions :

– le consentement exprès du payeur ;

– le payeur a initié l'opération pour le montant en question au moyen d'un instrument de paiement lié à une carte émis par le même prestataire de services de paiement ;

– l'authentification de l'émetteur auprès du gestionnaire du compte avant chaque demande de confirmation ;

– le respect des normes techniques de réglementation concernant la communication, émises par l'ABE, conformément à l'article 98.1 de la directive (voir *supra*).

Pour assurer la bonne information de l'utilisateur, l'article L. 133-39 prévoit également que le payeur peut demander au gestionnaire de son compte de lui communiquer l'identification de l'émetteur de l'instrument de paiement et la réponse qui lui a été transmise.

Sont exclues de l'application de ces dispositions les opérations de paiement initiées au moyen d'instruments de paiement liés à une carte sur lesquels est stockée de la monnaie électronique.

● La directive a choisi de maintenir l'exclusion des **opérateurs de distributeurs** de son champ d'application (article 3). Elle impose toutefois à ces derniers des exigences de transparence s'agissant de certains frais. Il en va ainsi des frais éventuellement appliqués lorsqu'est proposé un service de conversion monétaire, en vertu de l'article 59 de la directive, dont les dispositions ont été introduites dans le droit par le IV de l'article L. 314-7.

● L'exclusion des **« réseaux limités »** du champ de la directive de paiement fait l'objet d'une précision. Cette exclusion, issue de la directive 2007/64/CE, ne prenait pas en compte le fait que des volumes de paiement importants étaient couverts par ces réseaux limités. C'est la raison pour laquelle la directive DSP 2 dessine avec plus de précision les contours de la notion. L'article L. 521-3 du code monétaire et financier dispose désormais qu'une entreprise peut fournir des services de paiement, sans appartenir à la catégorie des prestataires de services de paiement, dès lors que les moyens de paiement utilisés ne sont acceptés :

– que dans les locaux de cette entreprise ou, dans le cadre d'un accord commercial avec elle, dans un réseau limité de personnes acceptant ces moyens de paiement ;

– que pour un éventail limité de biens ou de services.

La directive renforce également les obligations de déclaration de ces acteurs (article 37). Selon la nouvelle rédaction de l'article L. 521-3, ces entreprises de « réseaux limités », dont la valeur totale des opérations de paiement exécutées au cours des douze mois précédent excède 1 million d'euros, doivent préciser la nature des opérations à l'ACPR.

● Dans le même esprit, sont exclus du champ de la directive les services reposant sur des **instruments de paiement spécifiques**, qui peuvent être utilisés de manière seulement limitée. Cette notion recouvre notamment les cartes prépayées.

III. LES CONDITIONS D'EXERCICE DES SERVICES DE PAIEMENT

Les services de paiement sont soumis à des règles d'agrément ou d'enregistrement auprès des autorités nationales compétentes. La mission de supervision de ces services revient à l'ACPR. L'article 19 de l'ordonnance, modifiant l'article L. 612-2 du code monétaire et financier, lui permet de solliciter l'avis de la Banque de France, au titre de ses missions de surveillance de la sécurité de l'accès aux comptes de paiement.

A. LES RÈGLES D'AGRÉMENT ET D'ENREGISTREMENT

L'exercice des activités de fourniture de services de paiement est conditionné à l'obtention d'un agrément. La directive complète les conditions d'agrément et d'enregistrement et les adapte à l'apparition des PSIP et des PSIC (articles 11 à 16).

1. Des règles d'agrément complétées

● L'article 13 de l'ordonnance modifie ainsi l'article L. 522-6 afin de prendre en compte les nouvelles dispositions du droit européen. Il convient de noter que les PSIP, en tant qu'établissements de paiement, sont soumis à l'obligation d'agrément par l'ACPR, après avis de la Banque de France.

Tout d'abord, cet avis, qui portait sur le bon fonctionnement et la sécurité des systèmes de paiement, a été enrichi par l'ordonnance. Désormais, il doit également porter sur la **sécurité de l'accès aux comptes de paiement et à leurs informations dans le cadre de la fourniture de PSIP ou de PSIC**.

L'ACPR doit ensuite vérifier, en sus des conditions prévues dans la version du code antérieure à l'ordonnance, que l'établissement de paiement dispose de dispositifs « *à même d'assurer la sécurité des services de paiement fournis, ainsi que la protection des données de paiement sensibles* ».

Enfin, une condition « *d'honorabilité, de compétence et d'expérience nécessaires* » est ajoutée, comme le requiert l'article 5.1 de la directive.

L'article L. 522-6 confie à l'ACPR la mission d'apprécier le respect de cette condition.

L'article 11 de la directive a complété les conditions d'octroi de l'agrément en précisant que tout établissement de paiement doit exercer au moins une partie de son activité de prestation de services de paiement dans un État membre pour être agréé dans cet État membre. Le e) du 3° de l'article 13 de l'ordonnance applique ces dispositions au cas de la France, en modifiant l'article L. 522-8 du code monétaire et financier.

● Des conditions spécifiques d'enregistrement sont également instaurées. Conformément à l'article 14 de la directive, l'article 14 de l'ordonnance modifie l'article L. 523-4 du code monétaire et financier pour prévoir une **obligation d'enregistrement auprès de l'ACPR des agents** auxquels les prestataires de services de paiement entendent recourir. Selon la directive (article 19), ce registre est public. L'article L. 612-21 a donc été modifié pour transcrire cette obligation dans le code monétaire et financier.

2. L'agrément simplifié

Un **agrément simplifié** (article 32 de la directive) peut être délivré si les prestataires de services de paiement concernés exécutent des opérations dont la moyenne mensuelle de la valeur au cours des douze derniers mois n'excède pas une limite fixée par l'État membre qui, en tout état de cause, est inférieure à 3 millions d'euros. Ce critère doit être évalué par rapport au montant total prévisionnel des opérations de paiement.

L'article L. 522-11-1 prévoyait la possibilité de l'octroi d'un agrément « *limité* » dès lors que le montant total prévisionnel des opérations de paiement ne dépassait pas 3 millions d'euros, montant fixé par l'article D. 522-1-1 du code monétaire et financier. L'article 13 de l'ordonnance change la dénomination de cet agrément qui devient « *agrément simplifié* ». Délivré par l'ACPR, après avis de la Banque de France, comme l'agrément de droit commun, l'ordonnance prévoit que la demande d'agrément doit comporter une liste d'informations définie par arrêté [(1)]. Les conditions nécessaires à l'octroi de l'agrément sont précisées dans la loi :

– la présence de dispositifs propres à assurer la sécurité des services de paiement fournis par le prestataire de services et la protection des données de paiement sensible ;

– l'honorabilité, la compétence et l'expérience des dirigeants ;

– l'honorabilité des actionnaires.

---

(1) Cette liste a été fixée par l'article 2-1 de l'arrêté du 29 octobre 2009 portant sur la réglementation prudentielle des établissements de paiement créé par l'article 2 de l'arrêté du 31 août 2017.

En cas d'absence de refus de l'ACPR à une demande d'agrément simplifié, la loi prévoit que l'établissement est réputé agréé dans un délai fixé à trois mois par l'article R. 522-1 (1).

Les établissements bénéficiant de la procédure simplifiée ne sont pas soumis aux dispositions exigeant le respect de normes prudentielles. Ils ne peuvent pas exercer les activités de services de transmission de fonds, d'initiation de paiement et d'information sur les comptes. Leur sont toutefois applicables les obligations de droit commun concernant la protection des fonds.

3. Le retrait de l'agrément

Le régime de **retrait d'agrément** dans le droit national est réformé par la directive. L'ordonnance modifie l'article L. 522-11 afin d'ajouter aux cas pour lesquels l'ACPR peut retirer l'agrément qu'elle a octroyé celui où l'établissement de paiement omet de l'informer de changements majeurs relatifs aux conditions d'octroi de l'agrément, conformément à l'article 13 de la directive.

4. Le régime d'enregistrement applicable aux prestataires de services d'information sur les comptes

Les **PSIC** font l'objet d'un régime assoupli par rapport aux établissements de paiement. Ils ne sont pas soumis à un régime d'agrément à l'exercice de leur activité sur le territoire, mais à un **simple régime d'enregistrement** auprès de l'ACPR, prévu à l'article L. 522-11-2 du code monétaire et financier, créé par l'article 13 de l'ordonnance.

Néanmoins, avant d'enregistrer un PSIC, l'ACPR vérifie qu'il satisfait aux exigences suivantes :

– ses procédures de contrôle interne garantissent la sécurité des données ;

– il a souscrit à une assurance de responsabilité civile professionnelle ;

– son administration centrale se situe dans le même État que son siège statutaire ;

– ses dirigeants satisfont aux conditions d'honorabilité, de compétence et d'expérience.

De façon similaire au déroulement de la procédure d'agrément, l'absence de constat par l'ACPR que les conditions d'enregistrement ne sont pas remplies dans un délai de trois mois vaut enregistrement du prestataire.

---

(1) Dans sa version résultant de l'article 1er du décret n° 2017-1313 du 31 août 2017 portant transposition de la directive n° 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur.

Ces conditions doivent être constamment satisfaites et tout changement substantiel qui leur est relatif doit faire l'objet d'une déclaration.

L'ordonnance a prévu des cas de retrait des enregistrements par l'ACPR. Ces derniers peuvent être à la demande du prestataire ou d'office. Ils n'ont pas d'effet immédiat, celui-ci intervenant à l'issue d'une période déterminée par l'Autorité. À titre de sanction, l'ACPR peut également radier de la liste des PSIC un prestataire. L'arrêté du 31 août 2017 [(1)] a précisé les modalités de publication des décisions de radiation.

5. Les conditions d'exercice des établissements de monnaie électronique

La rénovation des règles de conditions d'exercice des services de paiement a également concerné les **établissements de monnaie électronique**. L'article L. 525-6 modifié par l'ordonnance prévoit une obligation

– de déclaration de ces établissements à l'ACPR, dès lors que la valeur totale de monnaie électronique excède 1 million d'euros ;

– d'actualiser annuellement cette déclaration et de justifier de la sécurité des moyens de paiement.

Ces établissements, conformément aux dispositions de la directive, peuvent, comme les établissements de paiement, fournir à titre de profession habituelle de services de paiement, mais également émettre et gérer de la monnaie électronique. Comme pour les autres établissements de paiement, l'avis que la Banque de France transmet à l'ACPR préalablement à la décision d'octroi ou non de l'agrément concerne également le système de sécurité d'accès aux comptes de paiement. L'article 2 de l'arrêté du 2 mai 2013 portant sur la réglementation prudentielle des établissements de monnaie électronique, dernièrement modifié par un arrêté du 31 août 2017, fixe la liste des documents que l'établissement doit fournir à l'ACPR dans le cadre de sa demande d'agrément.

Concernant la qualité du contrôle interne, la gouvernance et la protection des données, des exigences similaires à celles qui sont imposées aux autres établissements de paiement, sont applicables aux établissements de monnaie électronique, selon l'article L. 526-8, modifié par le 2° de l'article 16 de l'ordonnance. Elles sont toutefois adaptées « *aux caractéristiques et au volume de monnaie électronique émise et en circulation, ainsi qu'aux modalités de gestion et de distribution par l'établissement de monnaie électronique* ».

(1) Article 19-1 de l'arrêté du 29 octobre 2009 portant sur la réglementation prudentielle des établissements de paiement, créé par l'article 2 de l'arrêté du 31 août 2017 le modifiant.

B. LES CONDITIONS DE CAPITAL ET LE CONTRÔLE DE L'ACTIONNARIAT

1. Les conditions de capital

● Les établissements de paiement sont soumis à des règles de détention de capital. Elles concernent le capital initial : un montant minimal initial de 125 000 euros est exigé pour qu'un établissement de paiement puisse obtenir l'agrément. Ce montant est abaissé à 50 000 euros pour les établissements qui ne fournissent que des SIP et à 20 000 euros pour ceux qui fournissent exclusivement des services de transmission de fonds, selon l'article 7 de la directive. La fourniture de SIC n'entraîne pas d'exigence en termes de capital minimum, ce qui s'explique par la nature du service proposé. Rappelons qu'en outre, les PSIC ne sont pas des établissements de paiement.

Plus généralement, les fonds propres des établissements de paiement doivent respecter un niveau minimal à tout moment, selon l'article 8 de la directive. Cette règle n'est toutefois pas applicable aux PSIP et aux PSIC, conformément à l'article 9 de la même directive.

Le droit interne satisfaisait déjà aux exigences du droit européen à cet égard, bien que la création du statut juridique de SIP ait rendu nécessaires certaines précisions de rédaction. La section 3 du chapitre II du titre II du livre V du code monétaire et financier reprend ces exigences de capital initial et de fonds propres (articles L. 522-7, L. 522-14 et L. 522-15). Les seuils de capital minimum et la méthode de calcul des fonds propres applicables en droit interne sont identiques à ceux applicables en droit européen [(1)].

● L'article 16 de l'ordonnance est venu modifier l'article L. 526-30 du code monétaire et financier, pour prévoir que les établissements de monnaie électronique qui fournissant des services d'initiation de paiement sont soumis à l'exigence de capital minimum applicable à ce type de services.

2. Le contrôle de l'actionnariat

L'article 6 de la directive établit des règles de contrôle de l'actionnariat des établissements de paiement. Une obligation de notification aux autorités compétentes s'impose aux entreprises et particuliers qui acquièrent une participation dans un établissement de paiement, avec pour conséquence que leurs parts ou droits de vote atteindraient les seuils de 20 %, de 30 % ou de 50 %. Symétriquement, la même obligation s'applique aux entreprises et particuliers qui, du fait de la cession d'une partie des parts dans un établissement, verraient leur part dans le capital ou dans les droits de vote devenir inférieure à l'un des seuils précités.

---

(1) Articles 4 et 29 de l'arrêté du 29 octobre 2009 portant sur la réglementation prudentielle des établissements de paiement.

L'ordonnance transpose cette exigence de contrôle de l'actionnariat dans le droit interne. L'article L. 522-10-1, créé par l'article 13 de l'ordonnance, dispose qu'une opération de prise, d'extension ou de cession de participation, directe ou indirecte, dans un établissement de paiement, est soumise à un régime d'autorisation préalable de l'ACPR, dès lors qu'elle répond à des critères de seuils fixés par décret. Un arrêté du 31 août 2017 (1) les a fixés au même niveau que les exigences européennes.

En cas de non-respect de ces obligations, l'ACPR peut demander au juge de suspendre les droits de vote attachés aux actions qui auraient dû faire l'objet de l'autorisation. De même, lorsqu'il est passé outre le refus de l'ACPR d'autoriser l'opération, celle-ci peut demander au juge de suspendre les droits de vote qui y sont attachés.

C. DES AMÉNAGEMENTS AUX RÈGLES DE CUMUL D'ACTIVITÉS

● L'ordonnance aménage les règles de cumul d'activités des intermédiaires en financement participatif, pour tirer les conséquences de la création du statut de SPIC. Certains intermédiaires en financement participatif proposent des SIC. Soumis à des règles strictes concernant le cumul d'activités (article L. 548-1 et L. 548-2), il convenait d'opérer les modifications nécessaires pour que les SIC entrent de manière formelle dans le champ des activités qu'ils sont autorisés à exercer.

● L'article 18 de la directive détermine les cas où les établissements de paiement peuvent octroyer des crédits liés aux services d'exécution d'opérations de paiement pour lesquelles les fonds sont couverts par une ligne de crédit accordée à l'utilisateur et aux services d'émission d'instruments de paiement ou d'acquisitions d'opérations de paiement. Trois conditions cumulatives doivent être satisfaites pour qu'un établissement de crédit répondant aux conditions ci-avant puisse octroyer un crédit :

– le crédit doit avoir un caractère accessoire et doit être accordé uniquement dans le cadre de l'exécution d'une opération de paiement ;

– le crédit est remboursé dans un délai fixé par les parties, qui ne peut excéder douze mois ;

– le crédit n'est pas octroyé sur la base de fonds reçus ou détenus par l'établissement en vue de réaliser une opération de paiement ;

– l'établissement de paiement doit disposer à tout moment de fonds propres suffisants au regard du montant global de crédits octroyés.

---

(1) Arrêté du 31 août 2017 modifiant l'arrêté du 29 octobre 2009 portant sur la réglementation prudentielle des établissements de paiement.

L'article L. 522-2 reprend ces conditions, tout en renvoyant à un arrêté le soin de définir les conditions de fonds propres requises. L'arrêté du 31 août 2017 [(1)] a donc précisé que le montant de fonds propres est déterminé selon la méthode de l'approche standard du risque de crédit du règlement (UE) n° 575/2013 du Parlement européen et du Conseil du 26 juin 2013, au regard du montant global de crédits octroyés.

D. LA SUPERVISION DES ACTIVITÉS TRANSFRONTALIÈRES ET LA COOPÉRATION ENTRE LES AUTORITÉS DES ÉTATS MEMBRES

1. Le renforcement de la communication et de la coopération entre les autorités nationales compétentes

● Les articles 28 et 29 de la directive rénovent le cadre juridique applicable aux activités transfrontalières et à l'exercice de la liberté de prestation de services et du droit d'établissement. Dans ce cadre, la coopération entre les différentes autorités de supervision est renforcée. L'article 111 de la directive rend applicables ces dispositions aux établissements de monnaie électronique.

S'agissant de l'exercice du droit d'établissement d'un prestataire de services de paiement français souhaitant ouvrir une succursale à l'étranger, l'article L. 522-13, tel que modifié par l'ordonnance, maintient le **principe de communication d'informations par l'ACPR aux autorités compétentes de l'État membre d'accueil**.

Plusieurs dispositions sont ajoutées par rapport à la version antérieure. En premier lieu, l'établissement de paiement peut commencer son activité en s'établissant dans un autre État de l'Espace économique européen dès lors que sa succursale ou l'agent par l'intermédiaire duquel il s'établit sont enregistrés sur la liste prévue à cet effet. De même, dans le cas où l'établissement de paiement souhaite exercer son activité en vertu de la libre prestation de services, il peut le faire dès réception de la notification qu'il envoie à l'ACPR.

En deuxième lieu, l'article L. 522-13 dispose désormais que l'**ACPR peut refuser d'autoriser un établissement de paiement à exercer son activité dans un autre État** partie à l'Espace économique européen notamment sur la base des informations que les autorités de l'État d'accueil lui ont communiquées. Sur ce même fondement, une autorisation déjà octroyée peut être révoquée. En cas d'appréciations divergentes des autorités compétentes des États, une procédure de communication est instaurée entre ces autorités. Symétriquement, lorsque la France est l'État d'accueil d'établissements de paiement, l'ACPR évalue les informations que lui communique l'autorité compétente de l'État d'origine et lui communique toute évaluation défavorable ou toute information pertinente en lien avec la fourniture de services proposée.

---

(1) Arrêté du 31 août 2017 modifiant l'arrêté du 29 octobre 2009 portant sur la réglementation prudentielle des établissements de paiement.

En troisième lieu, l'ordonnance concrétise l'une des exigences de la directive en instaurant, pour les établissements de paiement souhaitant s'établir sur le territoire français, un **point de contact central,** en charge de la communication d'informations relatives au respect des dispositions du code monétaire et financier sur :

– les frais ou réduction pour l'usage d'un instrument de paiement donné ;

– les instruments de paiement et l'accès aux comptes ;

– les services de paiement ;

– les prestataires de services de paiement.

Il a pour objectif de faciliter la surveillance des autorités de supervision de l'État d'origine et de l'ACPR.

Cette innovation résulte de l'article 29 de la directive. Il renvoie toutefois à l'ABE le soin de déterminer des normes techniques de réglementation (NTR) d'application de ces dispositions. Les standards techniques sur le point de contact central au titre de la DSP2 (RTS CCP) ont été soumis par l'ABE à la Commission le 13 décembre 2018.

En quatrième et dernier lieu, l'ordonnance autorise les autorités compétentes de l'État d'origine de l'établissement de paiement qui s'est installé en France à **procéder à des inspections sur place de ses succursales**, après en avoir informé l'ACPR.

● L'article 20 de l'ordonnance rend également applicables les dispositions concernant l'échange d'information entre l'ACPR et les autorités compétentes des autres États membres dans le cadre du droit d'établissement et de la liberté de prestation de services aux établissements de monnaie électronique et aux PSIC.

2. Les mesures conservatoires dans des circonstances exceptionnelles

Lorsqu'un établissement de paiement ou un établissement de monnaie électronique ne se conforme pas à la réglementation, l'autorité compétente de l'État d'origine voit ses pouvoirs étendus par l'article 30 de la directive, dans des situations d'urgence où une action immédiate est nécessaire pour remédier à « *une menace grave pesant sur les intérêts collectifs des utilisateurs de services de paiement dans l'État d'accueil* ». Il leur est alors possible de **prendre des mesures conservatoires**, dans l'attente de mesures à prendre par les autorités compétentes de l'État membre d'origine. Ces mesures doivent être proportionnées et l'autorité compétente de l'État d'accueil doit, dans la mesure du possible, prévenir préalablement celle de l'État d'origine. Les 2° et 3° de l'article 20 de l'ordonnance ont traduit cette disposition dans le code monétaire et financier, en modifiant les articles L. 613-33-2 et L. 613-33-3.

3. Le régime de déclaration des agents

Le régime de déclaration des agents est modifié par l'article 14 de l'ordonnance. L'article L. 523-4 traite des obligations qui s'imposent aux établissements de paiement établis en France lorsque ceux-ci souhaitent recourir à un agent pour fournir des services de paiement dans un autre État partie à l'accord sur l'Espace économique européen. Avant l'entrée en vigueur de l'ordonnance du 9 août 2017, il était prévu que l'ensemble des établissements de paiement ayant leur siège social en France et souhaitant utiliser un agent pour exercer des activités

La rédaction de l'article issue de l'ordonnance distingue selon que l'établissement est un établissement de crédit ou un établissement de paiement.

Désormais, les prestataires de services de paiement autres que les établissements de crédit, ayant leur siège social en France et souhaitant recourir à des agents pour fournir des services de paiement dans un autre État de l'Espace économique européen, sont tenus de respecter les dispositions applicables en matière de droit d'établissement ou de liberté de prestation de services de l'article L. 522-13 présentées ci-dessus. Il en va de même pour les établissements étrangers souhaitant recourir à un agent pour fournir des prestations en France.

Les établissements de crédit souhaitant recourir à un agent pour fournir des prestations en France ont des obligations renforcées. Ils doivent informer l'ACPR de leur projet et lui présenter un certain nombre d'informations listées par l'arrêté du 31 août 2017 [(1)].

IV. LES DROITS ET OBLIGATIONS DES UTILISATEURS ET DES PRESTATAIRES DE SERVICES DE PAIEMENT

Partant du principe que les évolutions technologiques et de marché ont créé de nouveaux risques juridiques pour les utilisateurs des services de paiement, l'un des objectifs principaux de la directive DSP 2 a été de renforcer le niveau de protection des consommateurs dans l'utilisation de ces services. De manière plus générale, elle modifie les droits et obligations des utilisateurs et des prestataires.

A. L'AMÉLIORATION DES DROITS DES UTILISATEURS

Le 16° de l'article 2 de l'ordonnance modifie l'article L. 133-16 pour préciser que les conditions qui s'imposent à l'utilisateur de services de paiement s'agissant de la délivrance de l'instrument de paiement et de son utilisation doivent être **objectives, non discriminatoires et proportionnées**, comme le prévoit l'article 69 de la directive. Au-delà de ce principe général, les droits et obligations des utilisateurs font l'objet de modifications dans plusieurs domaines.

---

(1) Article 19 de l'arrêté du 29 octobre 2009 portant sur la réglementation prudentielle des établissements de paiement, dans sa rédaction issue de l'arrêté du 31 août 2017.

1. L'allégement de la responsabilité de l'utilisateur en cas d'opérations non autorisées

Les droits de l'utilisateur sont renforcés par **l'allégement de sa responsabilité en cas d'opérations non autorisées**, conformément à l'article 74 de la directive dont le 21° de l'article 2 de l'ordonnance tire les conséquences en modifiant l'article L. 133-19 du code monétaire et financier.

Tout d'abord, il abaisse de 150 à 50 euros le montant maximal à hauteur duquel l'utilisateur peut être responsable des pertes consécutives à la perte ou au vol d'un instrument de paiement. Il s'agit du cas typique de l'utilisation d'une carte de paiement volée avant que son utilisateur habituel fasse opposition sur cette carte.

Ensuite, il ajoute deux situations à la liste des cas où la responsabilité de l'utilisateur ne peut être engagée :

– la perte ou le vol ne pouvait être détecté par le payeur avant le paiement ;

– la perte résulte d'actes ou de carence du personnel d'un prestataire de services de paiement ou d'une entité vers laquelle ses activités ont été externalisées.

Enfin, il précise que le payeur ne supporte aucune conséquence financière si l'opération de paiement non autorisée a été effectuée sans que le prestataire de services de paiement du payeur n'exige une **authentification forte**, telle que prévue à l'article L. 133-44, sauf agissements frauduleux de la part du payeur. Dans le cas où le bénéficiaire ou son prestataire de services de paiement n'accepte pas une authentification forte, il lui revient de rembourser le préjudice financier causé au prestataire de services de paiement du payeur.

2. L'amélioration pour l'utilisateur des règles de dates de valeur et de blocage des fonds

● L'article 89 de la directive améliore les droits des utilisateurs en modifiant les règles concernant les **dates de valeur de corrections d'opérations mal exécutées**. La rédaction de l'article L. 133-22 du code monétaire et financier se conformait partiellement aux dispositions de l'article 89. Elle prévoyait déjà, en effet, que dans le cas d'une opération mal exécutée à cause du prestataire de services de paiement du payeur, celui-ci devait restituer le montant de l'opération au payeur. Le 23° de l'article 2 de l'ordonnance, modifiant l'article L. 133-22, ajoute que la date de valeur à laquelle le compte du payeur est crédité ne peut être postérieure à la date à laquelle il a été débité dans le cadre de l'opération.

Symétriquement, il était déjà prévu que dans l'hypothèse où la mauvaise exécution de l'opération soit imputable au prestataire de services du bénéficiaire, ce dernier doit mettre immédiatement à la disposition de son client le montant de l'opération. L'ordonnance vient préciser que la date de valeur à laquelle le compte est crédité ne peut être postérieure à la date de valeur qui aurait eu cours si l'opération avait réussi.

Suivant les dispositions de la directive, l'ordonnance ajoute à l'article L. 133-22 le cas des opérations exécutées tardivement, en ouvrant au prestataire de services de paiement du payeur la possibilité de demander au prestataire de services de paiement du bénéficiaire de veiller à ce que la date de valeur de crédit du compte ne soit pas postérieure à la date de valeur qui aurait été attribuée si l'opération avait été correctement exécutée.

● Des règles de date de valeur similaires sont introduites dans le droit interne par l'ordonnance, s'agissant d'**opérations initiées par le bénéficiaire ou par l'intermédiaire du bénéficiaire**, lorsque l'ordre de paiement n'a pas été transmis par le prestataire de services de paiement du bénéficiaire au prestataire de services de paiement du payeur (II de l'article L. 133-22).

Dans ce même type d'opérations, lorsqu'elles sont mal exécutées, l'article L. 133-22, dans sa version antérieure à l'ordonnance, reconnaissait le principe de responsabilité du prestataire de services de paiement du payeur, dès lors que celle du prestataire du bénéficiaire n'était pas engagée. Il lui revenait alors de restituer au payeur le montant de l'opération mal exécutée.

L'ordonnance vient y apporter une nuance en disposant que le prestataire de services de paiement du payeur est déchargé de cette obligation s'il apporte la preuve que le prestataire de services de paiement du bénéficiaire a reçu le montant de l'opération de paiement.

Enfin, l'ordonnance précise que, d'une part, les actions menées par le prestataire de services de paiement du payeur dans le cadre de son obligation de répondre favorablement à la demande de son client d'essayer de retrouver la trace de l'opération de paiement et, d'autre part, la notification du résultat de sa recherche à son client, s'effectuent **sans frais** pour celui-ci.

● S'agissant toujours des **opérations ordonnées par le bénéficiaire ou par son intermédiaire**, l'article L. 133-25 octroie au payeur un droit à un remboursement total **lorsque l'autorisation n'indique pas le montant de l'opération** et que celui-ci est supérieur au montant auquel le payeur pouvait raisonnablement s'attendre. Le 28° de l'ordonnance complète l'article L. 133-25 pour garantir que la **date de valeur** à laquelle le compte de paiement du payeur est crédité n'est pas postérieure à la date à laquelle il a été débité, conformément aux dispositions de l'article 76.1 de la directive. Ce droit au remboursement est inconditionnel dans le cas des prélèvements en euros [(1)] lorsque les prestataires de

(1) Il s'agit plus précisément des prélèvements visés à l'article 1er du règlement (UE) n° 260/2012 du Parlement européen et du Conseil du 14 mars 2012 établissant des exigences techniques et commerciales pour les virements et les prélèvements en euros et modifiant le règlement (CE) n° 924/2009.

services de paiement concernés sont situés dans l'Union, selon l'article L. 133-25-1 introduit par le 25° de l'article 2 de l'ordonnance. Le payeur et son prestataire peuvent toutefois convenir que ce droit au remboursement n'est pas applicable si le premier a consenti à l'exécution de l'opération directement auprès du second (article L. 133-25-2).

● L'amélioration des droits des utilisateurs des services de paiement concerne également les **opérations de paiement dont le montant n'est pas connu à l'avance**. Il n'est désormais plus possible pour le prestataire de services de paiement du payeur de bloquer les fonds sur son compte sans que celui-ci ait donné son consentement quant au montant exact à bloquer. Après réception de l'ordre de paiement et du montant à débloquer, il doit débloquer immédiatement les fonds. L'article 2 de l'ordonnance a introduit ces dispositions provenant de l'article 75 de la directive dans le code monétaire et financier, par la création des articles L. 133-42 et L. 133-43.

3. Les règles de mobilité et de bonne information

● La **mobilité du client** est favorisée, l'article 55 de la directive entendant donner aux utilisateurs de comptes bancaires la **faculté de résilier leur contrat-cadre de moins de six mois sans frais**. Fixé à douze mois dans le code monétaire et financier, le délai de résiliation a été abaissé à six mois par l'article 5 de l'ordonnance qui est venu modifier l'article L. 314-2. Il en va de même pour les conventions de compte de dépôt définies à l'article L. 312-1-1.

● Pour permettre la **bonne information des consommateurs** quant aux services de paiement disponibles et garantir un niveau de transparence du fonctionnement des établissements de paiement satisfaisant, l'article 14 de la directive prévoit que les États membres établissent un registre public dans lequel sont inscrits les prestataires de services de paiement agréés et leurs agents. L'article 19 de l'ordonnance a modifié l'article L. 612-21 afin de transposer cette disposition, dont les modalités d'application ont été précisées à l'article R. 612-20 [(1)].

B. LES DROITS ET OBLIGATIONS DES PRESTATAIRES

La directive (article 36) requiert des États membres qu'ils veillent à faire respecter le principe selon lequel les établissements de paiement doivent bénéficier d'un **accès objectif, non discriminatoire et proportionné aux services de comptes de paiement des établissements de crédit**. L'article L. 312-23 étend le champ des bénéficiaires du droit à un accès non discriminatoire aux établissements de monnaie électronique.

---

(1) Article modifié par l'article 1er du décret n° 2017-13-13 portant transposition de la directive n° 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur.

1. La mise en place de procédures de réclamation

L'amélioration des droits des utilisateurs des services de paiement se traduit concrètement par l'obligation pour les prestataires de services de paiement de mettre en place des **procédures de réclamation** efficaces sur le respect des règles fixées par la directive, en vertu de l'article 99 de ladite directive. Aux fins de transposition de ces dispositions, l'article 2 de l'ordonnance a introduit la section 16 « Traitement des réclamations » dans le code monétaire et financier. Elle contient l'unique article L. 133-45 qui reprend les dispositions de la directive régissant le déroulement de la procédure (articles 99 et 101).

La réponse du prestataire de services de paiement qui a fait l'objet de la réclamation doit aborder tous les points soulevés et doit être transmise dans les quinze jours ouvrables suivant la réception de la réclamation. Par dérogation à ce principe, dans les situations où il est impossible au prestataire de services de paiement de répondre dans les quinze jours, celui-ci est tenu d'envoyer une réponse d'attente, dans laquelle il motive le délai qui lui est nécessaire pour apporter une réponse au problème soulevé par la réclamation. En tout état de cause, cette réponse doit parvenir à l'utilisateur au plus tard trente-cinq jours ouvrables après la réception de la réclamation.

La **mise en place de ces procédures de réclamation** s'accompagne d'une exigence de bonne information du contribuable sur l'existence de procédures extrajudiciaires de règlement compétentes pour connaître des litiges touchant aux droits et obligations des prestataires de services de paiement. Des obligations de bonne information sont imposées au prestataire de services de paiement dans ce sens.

2. Les règles de disponibilité des fonds

Pour ce qui est des exigences de **disponibilité des fonds**, le 13° de l'article 2 de l'ordonnance ajoute une obligation aux prestataires de services de paiement, en modifiant l'article L. 133-14 du code monétaire et financier. Si l'obligation pour le prestataire du service de paiement du bénéficiaire de mettre à disposition du bénéficiaire le montant de l'opération immédiatement après que son propre compte a été crédité n'est pas nouvelle, l'ordonnance ajoute que cette obligation est applicable lorsque les opérations de paiement se déroulent au sein d'un même prestataire de services de paiement. L'extension de cette exigence est toutefois conditionnée à ce que l'opération ne nécessite pas de conversion de devises de sa part ou que la conversion qu'elle nécessite s'effectue entre les devises d'États membres de l'Union européenne. Cette évolution législative se conforme aux dispositions de l'article 87.2 de la directive.

3. Les règles applicables en matière de frais

● **En matière de frais**, les prestataires de services de paiement ne peuvent empêcher le bénéficiaire du paiement d'appliquer des frais, ou de proposer une réduction au payeur pour l'utilisation d'un instrument de paiement. Cette interdiction, découlant de l'article 62.3 de la directive, trouvait déjà une garantie à l'article L. 112-11 du code monétaire et financier, qui précise d'ailleurs que toute stipulation contraire à ce principe est réputée non écrite.

Le 1° de l'article 1er de l'ordonnance a toutefois modifié l'article L. 112-11 afin qu'il soit conforme en tout point à l'article 62.3, en y ajoutant,

– d'une part, qu'il est également interdit au prestataire de limiter la possibilité pour le bénéficiaire du paiement d'orienter de quelque manière que ce soit vers l'utilisation d'un instrument de paiement donné ;

– d'autre part, que les éventuels frais appliqués ne peuvent dépasser les coûts directs supportés par le bénéficiaire pour l'utilisation de l'instrument de paiement.

L'article 60 de la directive a aussi rendu nécessaire l'introduction de l'article L. 112-13 afin de prévoir que l'application de frais par les prestataires de services de paiement ou par les autres parties intervenant dans l'opération, au titre de l'utilisation d'un instrument de paiement, soit subordonnée à une obligation d'information de l'utilisateur de services avant l'initiation de l'opération.

Pour assurer le respect de ces dispositions, l'article 21 de l'ordonnance modifie l'article L. 511-7 du code de la consommation afin d'habiliter les agents de la concurrence, de la consommation et de la répression des fraudes à rechercher et constater les infractions ou manquement à celles-ci.

● Dans les cas de perte, de vol ou d'utilisation non autorisée d'un instrument de paiement ou des données qui lui sont liées, l'utilisateur de l'instrument de paiement doit en informer son prestataire, en vertu de l'article L. 133-17 du code monétaire et financier. Charge au prestataire de fournir les moyens adéquats pour permettre à l'utilisateur de se conformer à cette obligation. Afin de se conformer aux dispositions de l'article 70 de la directive, le 15° de l'article 21 de l'ordonnance a modifié l'article L. 133-15 en ajoutant que la fourniture de ces moyens permettant l'information de l'utilisateur à son prestataire doit s'effectuer **à titre gratuit**.

En revanche, comme le précise le IV de l'article L. 133-26, créé par le 30° de l'article 2 de l'ordonnance (transposant l'article 70.2 de la directive), le prestataire peut facturer à l'utilisateur les coûts de remplacement directement imputables à l'instrument de paiement.

● De même, lorsque le payeur procède à une **révocation d'un mandat** de prélèvement [(1)], le **prestataire de services de paiement ne peut imputer des frais** à l'utilisateur de services, selon le III de l'article L. 133-26, introduit par le 29° de l'article 2 de l'ordonnance.

Par dérogation à ce qui précède, il peut imputer des frais si, d'une part, le délai de révocation pour les prélèvements est forclos [(2)] et, d'autre part, la convention de compte de dépôt ou le contrat-cadre de services de paiement prévoit la possibilité d'imputer des frais.

● S'agissant de la **répartition des frais entre le bénéficiaire et le payeur**, l'article 62 de la directive dispose que chacun paie les frais prélevés par son prestataire de services dès lors que l'opération de paiement est effectuée à l'intérieur de l'Espace économique européen et que les deux prestataires de services (ou le prestataire de services lorsqu'un seul prestataire intervient) sont situés dans un État de l'Espace économique européen.

4. Les règles de responsabilité en cas d'opérations non exécutées ou mal exécutées

● En l'état du droit, dans le cas de la **mauvaise exécution d'une opération de paiement faisant suite à la fourniture par l'utilisateur d'un identifiant unique inexact**, le prestataire de services de paiement du payeur n'est pas responsable. Néanmoins, l'article L. 133-21 du code monétaire et financier le soumet à l'obligation de s'efforcer de récupérer les fonds engagés. Le 23° de l'article 2 de l'ordonnance, conformément à l'article 88 de la directive, complète l'article L. 133-21 en prévoyant que :

– le prestataire de services de paiement du bénéficiaire doit communiquer au prestataire de services de paiement du payeur toute information utile pour récupérer les fonds ;

– dans l'hypothèse où le prestataire de services de paiement du payeur ne serait pas parvenu à récupérer les fonds, le prestataire de services du payeur communique au payeur, à sa demande, toutes les informations utiles à la documentation d'un recours en justice.

● Comme il a été indiqué *supra*, l'article L. 133-23 du code monétaire et financier traite des cas où l'utilisateur **nie avoir autorisé une opération exécutée ou affirme que l'opération a été mal exécutée**. Si la directive a rendu nécessaire une modification du code monétaire et financier pour prendre en compte les paiements initiés par des PSIP, elle a de plus imposé un élargissement du champ

---

(1) Telle que définie par le règlement (UE) n° 260/2012 du Parlement européen et du Conseil du 14 mars 2012 établissant des exigences techniques et commerciales pour les virements et les prélèvements en euros et modifiant le règlement (CE) n° 924/2009.

(2) L'article L. 133-8 fixe l'expiration du délai à la fin du jour ouvrable précédant le jour convenu pour le débit des fonds.

des obligations que doivent respecter l'ensemble des prestataires de services de paiement. Cet article prévoyait déjà que le seul fait que l'opération a été dûment enregistrée n'emporte pas la preuve que le payeur l'a autorisée ou qu'il n'a pas satisfait, par négligence grave ou de manière intentionnelle, à ses obligations. Reprenant les termes de l'article 72 de la directive, le 26° de l'article 2 de l'ordonnance complète l'article L. 133-23 ajoute une précision : pour prouver la fraude ou la négligence grave de l'utilisateur, le **prestataire de services de paiement**, « *y compris le prestataire de services de paiement fournissant un service d'initiation de paiement* », **doit fournir des éléments,** sans plus de précisions sur leur nature.

5. Les obligations en matière de transmission d'information

Conformément au principe de proportionnalité, la directive impose des **obligations de transmission d'informations différenciées** selon les besoins des utilisateurs. Dans un souci d'efficacité, elle détermine toutefois des formes standards de communication.

Les exigences d'information fixées par la directive sont plus souples pour les opérations isolées que pour les opérations reposant sur un contrat-cadre déterminant les règles de multiples opérations.

Pour les premières, seules les informations essentielles doivent toujours être fournies sur l'initiative du prestataire de services de paiement. Cette souplesse s'explique par la présence, en général, du payeur au moment où il donne l'ordre de paiement. Les articles 44 et 45 de la directive disposent que le prestataire met à la disposition de l'utilisateur, « *sous une forme aisément accessible* », l'identifiant unique nécessaire à l'exécution de l'ordre de paiement, le délai d'exécution maximal et tous les frais attachés à l'opération. Toutefois, dès lors que l'utilisateur demande que ces informations lui soient communiquées sur support papier, le prestataire doit répondre favorablement à cette demande. Le 6° de l'article 6 de l'ordonnance du 9 août 2017 a transposé ces dispositions en modifiant l'article L. 314-11 du code monétaire et financier. Ce dernier renvoie désormais à un arrêté du ministre chargé de l'économie le soin de fixer la liste des informations à fournir.

6. Le régime des sanctions applicables

Afin de rendre effectives les obligations des prestataires découlant de cette directive, celle-ci renvoie aux États membres le soin de déterminer le **régime de sanctions applicables** (article 103). Suivant ces orientations, l'article 3 de l'ordonnance fixe le régime de sanctions en cas d'infractions aux règles suivantes :

– la transgression de l'interdiction faite au bénéficiaire d'appliquer des frais pour l'utilisation d'un instrument de paiement donné ;

– le manquement à l'obligation d'informer le payeur, qui s'impose au bénéficiaire d'un paiement, lorsqu'il propose une réduction au payeur pour l'utilisation d'un instrument de paiement donné.

V. LES EXIGENCES DE SÉCURITÉ POUR LES PAIEMENTS ÉLECTRONIQUES ET LA PROTECTION DES DONNÉES FINANCIÈRES

A. L'AUTHENTIFICATION FORTE

Comme il a été évoqué *supra*, les exigences de sécurité pour les paiements électroniques et la protection des données sont renforcées. Elles reposent sur le principe de **l'authentification forte du client**. Cette procédure d'identification consiste à vérifier l'identité de l'utilisateur en combinant plusieurs facteurs d'identification. Ces éléments d'identification doivent relever :

– de ce que seul l'utilisateur connaît (catégorie « connaissance ») ;

– de ce que seul l'utilisateur possède (catégorie « possession ») ;

– de ce que l'utilisateur est (catégorie « inhérence »).

Ce niveau d'authentification offre un niveau de sécurité bien supérieur au système d'authentification par simple mot de passe, qui est désormais insuffisant pour assurer la protection des informations sensibles.

Aux termes de l'article 97 de la directive, la procédure d'authentification forte du client devient obligatoire

– lorsqu'il accède à son compte ;

– lorsqu'il initie une opération de paiement électronique ;

– lorsqu'il exécute une action à distance, susceptible de comporter un risque de fraude.

Une garantie de sécurité supplémentaire est prévue pour les opérations de paiement électronique à distance. Pour ces types de paiement, l'authentification forte doit comporter des éléments qui établissent un **lien dynamique** entre l'opération, le montant et le bénéficiaire donnés.

L'article L. 133-44 introduit ces dispositions dans le code monétaire et financier. Il satisfait à l'exigence de l'article 97.4 aux termes duquel en prévoyant que les prestataires de services de paiement mettent en place les mesures de sécurité adéquates pour protéger la confidentialité et l'intégrité des données de sécurité personnalisées des utilisateurs.

Tout comme l'obligation pour les PSIP et les PSIC de s'identifier auprès du gestionnaire afin d'accéder aux données nécessaires à l'exercice de son activité, l'**obligation d'authentification forte n'entre en vigueur qu'une fois la période de transition expirée**, selon le VIII de l'article 34 de l'ordonnance.

Les NTR ne concernent en effet pas seulement les modalités d'accès des PSIP et des PSIC aux données bancaires des usagers, elles s'appliquent aussi à l'authentification forte des clients et à aux exigences auxquelles doivent satisfaire les mesures de sécurité afin de protéger la confidentialité et l'intégrité des données de sécurité personnalisée des utilisateurs. L'article 98.3 renvoie à l'acte réglementaire délégué de prévoir des dérogations qui reposent sur trois critères : le niveau de risque lié au service fourni ; le montant, le caractère récurrent de l'opération ou les deux ; le moyen utilisé pour exécuter l'opération.

Le projet de règlement de la Commission liste ces dérogations à son chapitre III. Elles concernent : l'accès à certaines informations autres que les données de paiement sensibles, le paiement sans contact au point de vente, certains automates de frais de parking ou de péage, les opérations récurrentes, les bénéficiaires de confiance, les virements entre comptes détenus par la même personne physique ou morale ; les opérations de faible valeur.

B. LE TRAITEMENT ET LA CONSERVATION DES DONNÉES

Plusieurs dispositions de la directive DSP 2 visent à améliorer la sécurité des données de paiement et des données personnelles. Le 5° de l'article 12 de l'ordonnance les a introduites dans la loi, aux articles L. 521-5 à L. 521-10 du code monétaire et financier.

● Conformément à l'article 94 de la directive, l'article L. 521-5 soumet ainsi le **traitement des données** à caractère personnel par les systèmes de paiement et les prestataires de services de paiement à la condition que ces traitements soient nécessaires à la prévention, la recherche et la détection des fraudes en matière de paiement. De plus, l'**accès**, le **traitement** et la **conservation** des données à caractère personnel sont conditionnés au **consentement explicite** de l'utilisateur. S'appuyant sur les compétences que lui confère le règlement général sur la protection des données [(1)] (RGPD), la Commission nationale de l'informatique et des libertés (CNIL) doit veiller au respect de ces deux dispositions (article L. 521-7). Avant le 25 mai 2018, date de l'entrée en vigueur du RGPD, la CNIL exerce cette mission au titre des compétences que lui reconnaît la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés [(2)].

● L'article L. 521-8 confie à la **Banque de France le soin d'assurer la sécurité de l'accès aux comptes de paiement et à leurs informations**, dans le cadre de la fourniture des services d'initiation de paiement et d'information sur les comptes. Dans l'exercice de cette mission, elle peut procéder aux expertises qui lui semblent utiles et peut se faire communiquer toute information pertinente.

---

(1) Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE.

(2) Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

● Pour gérer les risques opérationnels et de sécurité, la directive exige des États membres qu'ils veillent à ce que les prestataires de services de paiement établissent un **cadre prévoyant des mesures d'atténuation et des mécanismes de contrôle appropriés en vue de gérer les risques opérationnels** (article 95). L'article L. 521-9 traduit ces dispositions dans le droit interne. Le contenu même des procédures a été précisé par un arrêté du 31 août 2017 [(1)].

● S'agissant des **incidents**, la directive opère une distinction entre les incidents opérationnels et les incidents de sécurité (article 96). L'ordonnance prend le parti de distinguer l'autorité compétente à informer en cas d'incident majeur, selon qu'il s'agit d'un incident opérationnel ou de sécurité. Dans le premier cas, le prestataire devra en informer l'ACPR ; dans le second cas, il devra en informer la Banque de France, selon l'article L. 521-10. Dès réception de la notification, l'autorité compétente intéressée notifie les détails importants de l'incident à l'ABE et à la Banque centrale européenne (BCE).

Dans le cas où l'incident peut avoir un impact sur les intérêts financiers des utilisateurs de services de paiement, le prestataire doit en informer ses utilisateurs et les mesures envisagées pour limiter les conséquences de l'incident.

VI. LES DISPOSITIONS DE L'ORDONNANCE RELATIVES À L'APPLICATION DES RÈGLES DE LA DIRECTIVE EN NOUVELLE-CALÉDONIE, EN POLYNÉSIE FRANÇAISE ET À WALLIS-ET-FUTUNA

Conformément à l'habilitation de l'article 70 de la loi « Sapin 2 », l'ordonnance du 9 août 2017 a rendu applicables en Nouvelle-Calédonie, en Polynésie française et à Wallis-et-Futuna, les articles du code monétaire et financier, avec les adaptations nécessaires pour ceux qui relèvent de la compétence de l'État.

Les **articles 22 à 25 de l'ordonnance** modifient le titre IV du livre VII du code monétaire et financier relatif aux dispositions applicables à la **Nouvelle-Calédonie**. Les dispositions applicables à la **Polynésie française** et à **Wallis-et-Futuna** sont modifiées de la même façon, respectivement par **les articles 26 à 29 et 30 à 33 de l'ordonnance**. L'ordonnance procède à des simplifications rédactionnelles en présentant dans des tableaux les dispositions applicables.

Les adaptations nécessaires à l'application des dispositions de transposition de la directive dans ces territoires d'outre-mer sont les suivantes :

– les références en euros sont remplacées par des références en francs CFP et les montants exprimés en euros sont convertis en francs CFP ;

---

(1) Arrêté du 31 août 2017 modifiant l'arrêté du 2 mai 2013 portant sur la réglementation prudentielle des établissements de monnaie électronique.

– les règles de date de valeur en cas de remboursement par les prestataires de services de paiement du montant d'une opération mal exécutée aux utilisateurs ne sont pas applicables ;

– le délai d'exécution de l'opération de paiement est allongé à quatre jours ouvrables, contre trois jours ouvrables dans l'hexagone ;

– les références au droit de l'Union européenne ne sont pas applicables ;

– les dispositions de l'ordonnance concernant le droit commercial sont remplacées par des références au droit local ;

– les références à la Banque de France sont remplacées par les références à l'Institut d'émission d'outre-mer (IEDOM) ;

– les références au code civil sont remplacées par les dispositions en vigueur localement ayant le même effet ;

– les références aux dispositions du droit européen en matière de protection des données sont remplacées par des références au droit local applicable en la matière.

*
* *

*La commission **adopte** l'article 1er **sans modification**.*

*
* *

Après l'article 1er

La commission examine l'amendement CF7 de M. Jean-Noël Barrot.

M. Jean-Noël Barrot. À mon tour, je félicite et remercie Mme la rapporteure pour son travail sur ce texte très technique. Pour répondre à Jean-Louis Bourlanges, je voudrais remettre le sujet en perspective. Cette transposition vise à trouver un équilibre entre deux impératifs : la sécurité et la libération de l'innovation. Au niveau européen, la directive a donc été négociée entre les banques – qui ont essayé de s'assurer de la sécurisation des transferts d'information – et les nouveaux entrants – notamment les start-up – qui essaient d'offrir de nouveaux services d'information aux usagers et aux épargnants et ont besoin d'avoir accès aux données de ces derniers, avec leur accord bien entendu.

Dans le cadre de cette directive, les banques se sont engagées à mettre en place des API. Avec l'accord des usagers, elles permettront aux nouveaux entrants de se connecter à leurs comptes et d'utiliser ou, *a minima*, de mobiliser les données de manière plus sécurisée, par le biais des API, plus sûres que les pratiques actuelles. Des applications téléchargeables sur les téléphones portables existent déjà. Elles vous demandent vos identifiants afin d'aspirer vos données bancaires – avec votre accord –, et vous livrent des informations sur vos comportements de paiement et d'épargne.

La directive a restreint l'utilisation des API au compte courant des utilisateurs. Mon amendement vise, par parallélisme, à étendre ces dispositions aux comptes d'épargne, dans un triple objectif : tout d'abord, assurer aux utilisateurs le même niveau de sécurité pour leurs comptes d'épargne que pour leur compte courant, puisque la directive vise à assurer la sécurité des comptes des épargnants.

Par ailleurs, si les applications de ces start-up et entreprises de services de paiement ont accès aux comptes d'épargne, cela offrira une meilleure lisibilité aux épargnants sur leurs frais bancaires. Ces applications pourront vous dire quel pourcentage de votre budget vous avez consommé en alimentation, en transports, *etc.* Avec mon amendement, elles mettront également en lumière les frais que vous payez. Cela améliorera la visibilité des usagers sur les frais d'agios, mais également sur ceux liés aux différents produits d'épargne.

Enfin, mon amendement améliorera l'allocation de notre épargne, grâce au soutien de ces nouveaux fournisseurs de services. Ils pourront accompagner les Françaises et les Français, dont l'épargne sera ainsi plus naturellement fléchée vers des produits plus dynamiques et vers les entreprises. C'est un des objectifs poursuivis par le projet de loi relatif au plan d'action pour la croissance et la transformation des entreprises (PACTE).

Il me semble donc intéressant d'étendre le champ de la directive aux autres comptes d'épargne, quitte à faire éventuellement facturer ce service par les banques aux prestataires de services mobilisant ces données.

On pourra m'opposer le risque lié à l'extension du champ de la directive par la France seule. Mais il n'y a pas besoin d'attendre les autres pays européens pour améliorer la sécurité des épargnants français, la lisibilité des frais bancaires et l'allocation de l'épargne française. On peut simplement donner l'exemple en étendant le champ de la directive.

Mme la rapporteure. Je comprends parfaitement et partage la réflexion qui sous-tend cet amendement, mais je le prends comme un amendement d'appel. Sur la forme, il ne peut avoir les effets escomptés sans être précisé. Par ailleurs, sur le fond, la directive DSP2 ne concerne que les comptes de paiement, les comptes d'épargne ou d'assurance étant exclus de son champ. L'ordonnance qui nous est présentée transpose ces dispositions sans aller au-delà.

Vous avez tout à fait raison lorsque vous faites remarquer que les comptes agrégés, dans leur majorité, ne sont pas des comptes de paiement. Une partie du système sera donc régulée, avec des modalités d'accès encadrées, une autre partie ne l'étant pas. C'est pourquoi la question de l'extension du champ de la directive aux autres comptes se pose. Mais elle ne peut être réglée dans ce projet de loi : tout d'abord, il s'agirait d'une surtransposition – l'ordonnance ne peut pas aller au-delà de ce que prévoit la directive, M. le président l'a souligné. Par ailleurs, le Gouvernement évalue actuellement les normes internes surtransposant le droit européen. Nous devons donc réaliser un travail d'analyse plus approfondi de votre proposition. Ensuite, des discussions doivent s'engager avec les gestionnaires des comptes en question : il est important de consulter ces professions avant d'envisager l'application d'un cadre juridique portant à conséquences pour eux. Enfin et surtout, cette question doit être traitée au niveau européen, notamment pour des raisons de concurrence.

Je vous propose donc de retirer votre amendement.

M. Jean-Louis Bourlanges. Vous avez raison, on ne peut intégrer la proposition de Jean-Noël Barrot dans une transposition de directive. Mais elle a le mérite de poser une question de fond, celle de la subsidiarité, question sur laquelle nous devrions être actifs. Si le texte reste en l'état – Jean-Noël Barrot l'a très bien expliqué – le système est déséquilibré. Mais, si nous prenons une mesure unilatérale, cela crée une distorsion de concurrence, qui entre dans le champ de la subsidiarité.

Qu'est-ce que la subsidiarité ? Une décision doit être prise au niveau européen quand elle ne peut pas être traitée rationnellement au niveau national. En tant que Parlement, depuis le traité de Lisbonne, nous disposons d'un certain nombre de moyens d'action sur la Commission européenne. Nous devrions donc adresser à la Commission – qui a le pouvoir d'initiative – des messages d'appel solennels – je ne sais pas comment à ce stade, peut-être par le biais d'une résolution commune avec la commission des affaires européennes et un vote en séance publique de notre Assemblée. Si la Commission européenne a le monopole de l'initiative, rien ne nous empêche de transmettre une demande d'initiative.

Mme Véronique Louwagie. L'amendement proposé aboutirait à ce que s'applique en France, à des situations qui ne s'arrêtent pas à nos frontières, un dispositif unique en Europe. Par ailleurs, si, les uns et les autres, nous déplorons régulièrement des surtranspositions de directives, respectons donc en l'occurrence le principe, même s'il peut connaître des exceptions : ne surtransposons pas. Enfin, si un problème se pose, il faut l'aborder au niveau européen. Évaluons la mise en œuvre de cette directive et ses effets sur tous les acteurs, en termes tant d'offre de services que de sécurité globale du système, en prenant en compte l'évolution des menaces, probablement sans commune mesure aujourd'hui avec ce qu'elles étaient en 2015.

M. Jean-Noël Barrot. Je ne propose pas une surtransposition, je propose d'étendre le champ d'application des mesures transposées, ce qui est tout à fait possible.

Cela étant, ayant entendu les arguments de la rapporteure et d'autres collègues, je retire mon amendement. Il n'en serait pas moins intéressant que le débat lancé par Jean-Louis Bourlanges ait lieu en séance.

M. le président Éric Woerth. Effectivement, vous pouvez redéposer votre amendement en vue de la séance car le débat mérite d'avoir lieu.

L'amendement CF7 est ***retiré.***

Article 2
(articles L. 133-1, L. 133-2, L. 133-28, L. 133-3,
L. 133-40 et L. 133-41 du code monétaire et financier)
Corrections apportées aux dispositions de l'ordonnance relatives aux instruments de paiement et à l'accès aux comptes

Le 1° de l'article 2 modifie l'article L. 133-1 du code monétaire et financier, relatif au champ d'application des règles applicables aux instruments de paiement et à l'accès aux comptes, pour préciser que les opérations de paiement effectuées entre prestataires de services de paiement pour leur propre compte n'y étaient pas soumises. Il réintroduit l'ancien III de l'article, supprimé inopportunément par l'ordonnance. Cette exclusion découle directement de l'article 3 de la directive.

Le 2° procède à une coordination à l'article L. 133-2 qui n'avait pas été réalisée par l'ordonnance. Elle est rendue nécessaire par la modification de l'article L. 133-7.

Le 3° modifie l'article L. 133-28 qui prévoit des possibilités de déroger au droit commun pour des opérations de faibles montants. Il propose de permettre au payeur et au prestataire de services de paiement, si l'instrument de paiement a été utilisé de manière anonyme ou si le prestataire n'est pas en mesure de prouver qu'une opération a été autorisée, de déroger par contrat aux deux règles suivantes :

– l'absence de conséquence financière pour le payeur qui a perdu ou s'est fait voler son instrument de paiement et a prévenu son prestataire de services de paiement pour qu'il le bloque ;

– l'obligation pour le PSIP de prouver que l'ordre de paiement a été reçu par le gestionnaire et correctement exécuté, dans le cas où l'utilisateur nie avoir exécuté l'opération ou affirme qu'elle a été mal exécutée.

Ces dispositions transposent le point b) de l'article 63 de la directive.

Les 4° à 8° opèrent des modifications rédactionnelles.

La rapporteure propose d'adopter cet article moyennant un amendement rédactionnel.

*
* *

*La commission **adopte** l'amendement rédactionnel CF1 de la rapporteure.*

*Puis elle **adopte** l'article 2 **modifié**.*

*
* *

Article 3
(articles L. 522-3, L. 522-8, L. 522-13, L. 525-9, L. 526-19, L. 526-24, L. 526-28 et L. 561-2 du code monétaire et financier)
Correction d'une erreur de référence à l'article L. 351-1 du code monétaire et financier

L'article 3 du projet de loi propose de corriger une erreur de référence, les alinéas de l'article L. 312-1-1 du code monétaire et financier, visés par l'article L. 351-1 du code monétaire et financier, n'ayant pas pris en compte les modifications apportées par l'ordonnance du 9 août 2015.

La correction proposée ne prend toutefois pas en compte la rédaction de l'article L. 312-1-1 qui entrera en vigueur le 1er avril 2018 (1).

La rapporteure propose donc d'amender cet article pour prendre en compte la rédaction à venir de l'article L. 312-1-1.

*
* *

*La commission **adopte** l'amendement rédactionnel CF2 de la rapporteure.*

*Puis elle **adopte** l'article 3 **modifié**.*

*
* *

(1) Rédaction qui résultera de l'article 16 de l'ordonnance n° 2017-1433 du 4 octobre 2017 relative à la dématérialisation des relations contractuelles dans le secteur financier.

Article 4

Dispositions de coordinations et corrections de rédaction au titre II du livre V du code monétaire et financier

Cet article opère des coordinations de références aux articles L. 522-3 et L. 526-28.

Il améliore la rédaction des articles L. 522-8, L. 522-13 et L. 526-24.

Il corrige des erreurs de référence aux articles L. 526-9, L. 526-19 et L. 561-12.

La rapporteure propose des modifications rédactionnelles supplémentaires.

*
* *

*La commission **adopte** l'amendement rédactionnel CF3 de la rapporteure.*

*Puis elle **adopte** l'article 4 **modifié**.*

*
* *

Article 5
(article L. 612-2 du code monétaire et financier)
Correction d'une erreur de rédaction concernant les compétences de l'Autorité de contrôle prudentiel et de résolution

Une erreur de rédaction à l'article 19 de l'ordonnance du 9 août 2015 a conduit à supprimer l'alinéa de l'article L. 612-2 du code monétaire et financier aux termes duquel le contrôle de l'ACPR sur l'activité de prestation de services d'investissement des établissements de crédit et des entreprises d'investissement ou des entreprises de marché [(1)] s'exerce sous réserve de celle de l'Autorité des marchés financiers en matière de contrôle des règles de bonne conduite et autres obligations professionnelles.

L'article 5 du projet de loi remédie à cette erreur.

La rapporteure propose des ajustements rédactionnels.

*
* *

*La commission **adopte** l'amendement rédactionnel CF4 de la rapporteure.*

*Puis elle **adopte** l'article 5 **modifié**.*

*
* *

(1) Il s'agit des personnes mentionnées aux 1° et 2° de l'article L. 612-2 du code monétaire et financier.

Article 6

(articles L. 741-2-1 A, L. 751-2-1 A, L. 753-2, L. 753-3, L. 753-7-1, L. 743-3, L. 743-7-1, L. 745-8, L. 745-8-1, L. 745-13, L. 746-2, L. 755-8-1, L. 755-13, L. 756-2, L. 761-1-2 A, L. 763-3, L. 763-7-1, L. 765-8-1, L. 765-13 et L. 766-2 du code monétaire et financier)

Dispositions de coordinations et corrections d'erreurs de rédaction relatives à l'application de l'ordonnance n° 2017-1252 du 9 août 2015 en Nouvelle-Calédonie, en Polynésie française et à Wallis-et-Futuna

Les dispositions du présent projet de loi rendent nécessaires des coordinations dans les articles prévoyant les règles d'application et les adaptations requises en Nouvelle-Calédonie, en Polynésie-française et à Wallis-et-Futuna.

● Le présent article modifie les articles L. 741-2-1 A, L. 751-2-1 A et L. 761-1-2 A, L. 753-2, L. 743-7-1, L. 753-7-1, L. 763-7-1, L. 745-8-1, L. 765-7-1, L. 745-13, L. 755-13, L. 765-13, L. 746-2, L. 756-2 et L. 766-2 afin d'actualiser la liste des dispositions de l'ordonnance applicables aux territoires mentionnés ci-avant.

Des simplifications de rédaction sont notamment apportées concernant les **règles de champ d'application de l'ordonnance** : ses dispositions relatives aux instruments de paiement, à l'accès aux comptes et aux services de paiement sont applicables dans ces territoires d'outre-mer si le prestataire de services de paiement du bénéficiaire et celui du payeur sont situés sur le territoire de la République et que l'opération est réalisée en euros ou en francs CFP. Dans le droit commun, ces dispositions s'appliquent lorsque l'un au moins des prestataires est situé en France hexagonale et l'autre dans un État partie à l'Espace économique européen. Les règles d'extraterritorialité de l'ordonnance qui ont cours lorsque l'un au moins des prestataires de paiement se situe dans l'Espace économique européen ne s'appliquent pas aux territoires en question.

● Deux erreurs matérielles sont corrigées :

– le tableau des articles L. 743-7-1, L. 753-7-1 et L. 763-7-1 vise l'article L. 313-14 au lieu de l'article L. 314-14 ;

– les articles L. 745-13, L. 755-13 et L. 765-13 visent l'article L. 565-25 au lieu de l'article L. 565-24.

● Une omission de référence à l'article L. 745-8 est réparée.

*

* *

*La commission **adopte** l'amendement rédactionnel CF5 de la rapporteure.*

*Puis elle **adopte** l'article 6 **modifié**.*

*Elle **adopte** ensuite l'ensemble du projet de loi **modifié**.*

*

* *

ANNEXE N° 1 :
LISTE DES PERSONNES AUDITIONNÉES PAR LA RAPPORTEURE

Fédération bancaire française *

– M. Benoît de la Chapelle Bizot, directeur général délégué

– M. Jérôme Raguenes, directeur du département numérique, systèmes et moyens de paiement

– M. Nicolas Bodilis Reguer, directeur du département relations institutionnelles

France Fintech

– M. Joan Burkovic, directeur général de Bankin

Direction générale du Trésor

– M. Arnaud Delaunay, chef du bureau services bancaires et moyens de paiement

– M. Jérémy Giglione, adjoint au chef du bureau services bancaires et moyens de paiement

– M. Emmanuel Monnet, conseiller financement de l'économie

***** Ces représentants d'intérêts ont procédé à leur inscription sur le registre de la Haute Autorité pour la transparence de la vie publique.

ANNEXE N° 2 :
LISTE DES PERSONNES AYANT FOURNI UNE CONTRIBUTION ÉCRITE

Mercatel

– M. Jean-Michel Chanavas, délégué général

Agence nationale de la sécurité des systèmes d'information (ANSSI)

– M. Guillaume Poupard, directeur général

Banque de France

Société Glory